# The Business Premium activation check

20 security controls you already pay for, and how to tell whether they're on

Microsoft 365 Business Premium includes enterprise-grade protection for identities, devices, email, files, and data. Most of it ships switched off, and it stays off, because turning it on means working through six admin centers and your DNS registrar, and Microsoft shipped more than 50 changes to Entra, Intune, and Defender last year that don't switch themselves on.

This check takes about 30 minutes. You need a Global Reader role (or Security Reader plus the SharePoint and Teams admin roles). It changes nothing. Score one point per control that is on.

### How to read the score

| Score | What it usually means |
|---|---|
| 0–8 | The tenant is running on defaults. Most of the license value is still in the box. |
| 9–15 | Someone did a security project once. Check the dates; a project is a snapshot. |
| 16–20 | Somebody operates this tenant. The question becomes who keeps it there next year. |

## Identity (Microsoft Entra ID P1)

**1. MFA is required for every user.** Where: Entra admin center → Protection → Conditional Access → Policies (or Identity → Overview → Properties → Security defaults). On looks like: a policy that requires multifactor authentication for **all users and all resources**, with only an emergency-access account excluded — or security defaults enabled and no per-user exceptions. Off looks like: MFA "registered" but not required, or a policy scoped to a pilot group that never grew.

**2. Legacy authentication is blocked.** Where: Conditional Access → Policies → look for a "Block legacy authentication" policy; then Monitoring → Sign-in logs, filter Client app to the legacy protocols. On looks like: the policy is On (not report-only) and the legacy sign-in count is zero. Why it matters: older protocols cannot do MFA, which is why most compromised sign-ins use them.

**3. Admin accounts are few, cloud-only, and protected.** Where: Entra → Roles & admins → Global Administrator. On looks like: two to four Global Administrators (Microsoft's guidance is fewer than five), each a separate admin account rather than a daily-use mailbox, MFA required, and one documented emergency-access account that is excluded from Conditional Access and monitored.

**4. Access requires a compliant device (or MFA on unmanaged devices).** Where: Conditional Access → Policies → look for "Require device to be marked as compliant". On looks like: a policy for all users and all resources that requires a compliant device, or a compliant device *or* MFA, backed by the Intune compliance policies in control 7.

**5. Self-service password reset and banned passwords are on.** Where: Entra → Protection → Password reset → Properties; Entra → Protection → Authentication methods → Password protection. On looks like: self-service reset enabled for all users; custom banned password list enforced (your organization's name, town, and acronyms in it).

---

## Devices (Microsoft Intune Plan 1 and Microsoft Defender for Business)

**6. Laptops and phones are enrolled in Intune.** Where: Intune admin center → Devices → All devices. On looks like: the device count roughly matches headcount, and every laptop that touches company data appears here. Off looks like: a handful of enrolled devices and the rest managed by nobody.

**7. A compliance policy exists for each platform, and non-compliance has consequences.** Where: Intune → Devices → Compliance → Policies. On looks like: policies for Windows, macOS, iOS, and Android that require encryption, a minimum OS version, and an active antimalware service, with actions for non-compliance, and control 4 enforcing them.

**8. Defender for Business is onboarded on every device.** Where: Defender portal → Assets → Devices; Intune → Endpoint security → Endpoint detection and response. On looks like: every managed device shows as onboarded with an active sensor. This is the endpoint detection and response your cyber-insurance questionnaire asks about.

**9. Attack surface reduction rules are in block mode.** Where: Intune → Endpoint security → Attack surface reduction. On looks like: the core rules (for example, blocking Office apps from creating child processes and blocking executable content from email) set to Block, not Audit or Off.

**10. Disk encryption is enforced and keys are escrowed.** Where: Intune → Endpoint security → Disk encryption. On looks like: BitLocker required on Windows and FileVault on macOS, with recovery keys stored in Entra — so a lost laptop is a hardware loss, not a data breach.

**11. App protection policies cover company data on personal phones.** Where: Intune → Apps → App protection policies. On looks like: Outlook, Teams, and OneDrive on iOS and Android require a PIN, block saving to personal storage, and can be wiped selectively when someone leaves.

---

## Email (Microsoft Defender for Office 365 Plan 1)

**12. The Standard or Strict preset security policy is assigned to everyone.** Where: Defender portal → Email & collaboration → Policies & rules → Threat policies → Preset security policies. On looks like: Standard (or Strict) applied to all recipients. Microsoft turns these off until you turn them on; without them you are running the built-in baseline, not the Defender for Office 365 protection you licensed (Safe Links, Safe Attachments, tuned anti-phishing).

**13. Impersonation protection names your executives and your domains.** Where: Threat policies → Anti-phishing → the policy that applies to everyone → Impersonation. On looks like: the executive director, CEO, CFO, and anyone who approves payments listed under "users to protect"; your domains under "domains to protect"; mailbox intelligence on. This is the control that flags a message from a free mailbox carrying your ED's name. It is not enabled by default.

**14. SPF, DKIM, and DMARC are published for every domain that sends mail.** Where: Defender portal → Email authentication settings → DKIM (per domain); your DNS registrar for the SPF and DMARC records. On looks like: SPF ending in `-all`; DKIM enabled for each custom domain; a DMARC record at `_dmarc.yourdomain` with a reporting address and a policy of `quarantine` or `reject`. `p=none` means you are monitoring, not stopping. No record means anyone can send as you and receivers can't tell.

**15. Auditing is on and someone can search it.** Where: Purview portal → Audit. On looks like: audit search returns results for the last 90 days, and mailbox auditing is on. If nobody has ever run a search, treat it as off in practice.

---

## Collaboration (SharePoint, OneDrive, Teams)

**16. External sharing is set on purpose, not by default.** Where: SharePoint admin center → Policies → Sharing. On looks like: the organization-level setting is "New and existing guests" (or stricter) unless a deliberate decision says otherwise; "Anyone" links expire and are view-only; the default link type is "Specific people" or "Only people in your organization". Microsoft's defaults allow external sharing and set OneDrive to "Anyone".

**17. Teams external access and guest access have been reviewed.** Where: Teams admin center → Users → External access, and → Guest access; Entra → External Identities → External collaboration settings. On looks like: external access limited to the domains you actually work with (Microsoft's default allows all domains); guest invitations limited to admins or a defined group; a guest review at least yearly.

## Data (Microsoft Purview, Business Premium subset)

**18. Sensitivity labels are published.** Where: Purview → Information protection → Labels and Label policies. On looks like: a starter set (for example, General, Internal, Confidential) published to all users with a default label. This is one of the two foundations Microsoft 365 Copilot inherits on day one.

**19. A data loss prevention policy covers the data you would least like to see leave.** Where: Purview → Data loss prevention → Policies. On looks like: at least one policy for the sensitive information types that matter to you (financial account numbers, Social Security numbers, health information) across Exchange, SharePoint, OneDrive, and Teams — in test mode with notifications is a pass; nothing configured is not.

## Operating discipline

**20. Secure Score is reviewed monthly and Microsoft's changes are owned by someone.** Where: Defender portal → Secure Score; Microsoft 365 admin center → Message center. On looks like: the score and its trend reviewed at least monthly, improvement actions assigned to a named person, and Message center posts triaged. This is the control that keeps the other 19 on. Without it, the score above is a photograph, and it fades.

## What this check cannot tell you

Whether the settings that are on are *right* for your organization — the exceptions, the service accounts, the sharing that a grant workflow actually needs, the Conditional Access design that keeps the board's devices working. That is the next conversation, not this document.

## What to do with the number

- **16–20:** keep whoever is operating the tenant, and ask them for the exception log.
- **9–15:** find out the date of the last project, then run this check again in 90 days. If the score drops, the problem is drift, not the project.
- **0–8:** the value you are paying Microsoft for is still in the box. The direct path is a mapped picture of every control against this list. That is what Centered Networks' Readiness Assessment produces; if you would rather do it yourself, every "Where" line above is the starting point, and Microsoft's own guidance for Business Premium is at learn.microsoft.com under "Microsoft 365 Business Premium security".

*Centered Networks · Microsoft Solutions Partner · PO Box 1801, Ennis, MT 59729-1801 · centerednetworks.com*