always online

TECHNOLOGY GUIDE · IDENTITY & ENDPOINT SECURITY

Defender for Business & Conditional Access

the perimeter is who you are and what you sign in from

www.whedoit.com · always online

warren@whedoit.com · 0421 346 887

A guide for business owners and IT leads: how Conditional Access and Microsoft Defender for Business work together, what whedo.it configures, what Business Premium does and doesn't include, and how a roll-out works without locking anyone out.

1. Two halves of the same job

Conditional Access is Microsoft's Zero Trust policy engine. At its simplest, a policy is an if-then statement: if a user wants to reach a resource, then they must meet a condition, such as completing MFA or using a compliant device. It brings together signals about the user, location, device, application and risk to make that decision.

Microsoft Defender for Business protects the devices themselves: next-generation protection, endpoint detection and response, attack surface reduction, automated investigation and remediation, and vulnerability management, across Windows, Mac, iOS/iPadOS and Android.



Sign-in security decides who gets in; endpoint security protects what they sign in from.

2. Conditional Access signals and decisions

Signal	Example use
User or group	Apply stricter rules to administrators than to everyone else.
Location (IP)	Allow or block sign-ins from IP ranges, or from whole countries or regions.
Device	Require a device that Intune reports as compliant.
Application	Apply different rules when users open specific apps.
Risk	Respond to risky sign-ins or users (needs Entra ID P2).

The decision is either **block access**, or **grant access** with conditions such as MFA, a stronger authentication method, a compliant device, an approved client app, an app protection policy or a password change.

3. What whedo.it configures

Area	Typical default	whedo.it standard
Sign-in	Security defaults or passwords only; legacy authentication allowed	Conditional Access: MFA for all users, legacy authentication blocked, device-compliance and named-location rules
Devices	Defender on, untuned	Defender for Business onboarded and tuned as the active antivirus, attack surface reduction rules, BitLocker and update rings through Intune
Detection & response	Alerts unwatched	Acronis EDR with a 24/7 MDR security operations centre layered over Defender
Email	Standard anti-spam	Safe Links, Safe Attachments, anti-phishing and impersonation protection, SPF, DKIM and DMARC
Posture	Drifts as Microsoft changes	Monitored and kept tightened



Every managed device is protected and reports its health back to sign-in policy.

4. What Business Premium includes, and what it doesn't

- **Included:** Entra ID P1 (with Conditional Access), Defender for Business, Defender for Office 365 Plan 1 and Intune Plan 1.
- **Not included:** Entra ID P2 features such as risk-based Conditional Access and Privileged Identity Management, and Defender for Business protection for servers, which needs extra licences.
- We tell you when a P2 or server add-on is worth it for your risk, and we don't assume it's there when it isn't.

5. Rolling it out without locking anyone out

Step	What happens
1. Review	We record current sign-in methods, admin accounts, legacy authentication use and device state.
2. Prepare	Users register MFA methods; break-glass admin accounts are set up and excluded from policies.
3. Report-only	Policies run in report-only mode first so we can see who would be blocked.
4. Enforce	Policies are switched on in stages, starting with administrators.
5. Devices	Defender for Business onboarded and tuned; Acronis EDR and MDR in place.
6. Watch	Alerts and posture monitored, with policies adjusted as the business changes.

6. Common questions

We already have MFA. Isn't that enough? MFA is essential, but Conditional Access also blocks legacy sign-in methods that bypass MFA, and can require a healthy device as well as the right person.

Does Defender for Business replace our antivirus? Defender for Business is the active antivirus and endpoint protection in our standard, with Acronis EDR and MDR layered over it.

SOURCES

Microsoft Learn: Microsoft Defender for Business overview (learn.microsoft.com/defender-business/mdb-overview) · Microsoft Learn: What is Conditional Access? (learn.microsoft.com/entra/identity/conditional-access/overview) · Microsoft Learn: Enforce MFA using Conditional Access (security defaults note) (learn.microsoft.com/azure/virtual-desktop/set-up-mfa) · Microsoft Learn: Microsoft Defender for Office 365 overview (learn.microsoft.com/defender-office-365/mdo-about) · Microsoft Learn: Microsoft 365 Business Premium security overview (learn.microsoft.com/microsoft-365/admin/security-and-compliance/m365b-security-overview)

always online

whedo.it

always online

www.whedoit.com

warren@whedoit.com

0421 346 887

whedo.it Pty Ltd ATF whedo trust

ABN 32 457 075 010 · Perth, WA