Windows 11 w firmie 2026 — przegląd zmian i mapa „co gdzie”

Typ: fiszka **Poziom: średniozaawansowany**
Dotyczy: Windows 11 24H2/25H2/26H1, domena AD z GPO, Intune **Czas: ~30 min**

Efekt: wiemy, co w latach 2024–2026 zmieniło się w administrowaniu flotą Windows 11 w domenie, które terminy są twarde, gdzie w GPO i w Intune leży każde z ustawień i która strona tego rozdziału prowadzi przez wykonanie. Historię i kontekst tych zmian opowiada strona serii o Windows 11; tu jest wyłącznie warstwa robocza.

Skróty użyte na tej stronie (57)

Skrót	Co znaczy
AD	Active Directory: katalog kont, komputerów i zasad w domenie Windows
ADMX	szablony administracyjne zasad grupy w formacie XML
AI	Artificial Intelligence: sztuczna inteligencja
AVD	Azure Virtual Desktop: pulpity i aplikacje Windows uruchamiane w chmurze Azure
CA	Certificate Authority: urząd certyfikacji, który podpisuje inne certyfikaty
CDP	Connected Devices Platform: usługa łącząca urządzenia i synchronizująca aktywność
CFR	Controlled Feature Rollout: stopniowe włączanie funkcji partiami urządzeń
CIS	Center for Internet Security: organizacja publikująca bazy utwardzania systemów
CSP	Configuration Service Provider: interfejs ustawień Windows sterowany przez MDM, np. Intune
CSV	Comma-Separated Values: tabela w pliku tekstowym, kolumny rozdzielone przecinkami
DBX	baza sygnatur zakazanych w Secure Boot, czyli lista odwołań (zmienna UEFI dbx)
DLP	Data Loss Prevention: oprogramowanie pilnujące, by dane nie wyciekły z firmy
DoD	Department of Defense: chmura Microsoftu dla Departamentu Obrony USA
EDR	Endpoint Detection and Response: agent wykrywający i blokujący ataki na stacji

Skrót	Co znaczy
EOG	Europejski Obszar Gospodarczy: UE oraz Islandia, Liechtenstein i Norwegia
EPM	Endpoint Privilege Management: płatny dodatek Intune do kontrolowanego podnoszenia uprawnień
ESP	Enrollment Status Page: ekran postępu konfiguracji urządzenia przy rejestracji w Intune
ESU	Extended Security Updates: płatne poprawki bezpieczeństwa po końcu wsparcia
GCCH	GCC High: wydzielona chmura Microsoftu dla administracji USA
GPO	Group Policy Object: obiekt zasad grupy w Active Directory
GPT	GUID Partition Table: nowoczesny układ partycji dysku, wymagany przez rozruch UEFI
HTML	HyperText Markup Language: język stron WWW
HVCI	Hypervisor-protected Code Integrity: w interfejsie „Integralność pamięci”; sprawdza sterowniki przed jądrem
IoT	Internet of Things: urządzenia wbudowane i specjalizowane, np. kioski i terminale
IPP	Internet Printing Protocol: standardowy protokół druku sieciowego
ISO	obraz płyty instalacyjnej w formacie ISO 9660
KB	Knowledge Base: numer artykułu i aktualizacji Microsoftu (np. KB5124008)
KEK	Key Exchange Key: klucz UEFI autoryzujący zmiany baz DB i DBX
LAPS	Local Administrator Password Solution: automatyczna rotacja haseł lokalnych administratorów
LOB	Line of Business: aplikacja biznesowa firmy, pakowana do wdrożenia
LSA	Local Security Authority: podsystem Windows obsługujący logowanie i sekrety
LTSC	Long-Term Servicing Channel: wydanie z długim wsparciem i bez nowych funkcji
MAK	Multiple Activation Key: klucz aktywacji wielu urządzeń w licencjonowaniu zbiorowym
MDM	Mobile Device Management: zdalne zarządzanie urządzeniami, np. przez Intune
MDT	Microsoft Deployment Toolkit: darmowe narzędzie do wdrażania obrazów Windows
MSI	Microsoft Installer: format pakietu instalacyjnego Windows
NTLM	NT LAN Manager: starszy protokół uwierzytelniania Windows, poprzednik Kerberosa w domenie
OOBE	Out-of-Box Experience: kreator pierwszego uruchomienia Windows
PC	Personal Computer: komputer osobisty
PCA	Production Certificate Authority: urząd podpisujący produkcyjne pliki rozruchowe Windows
PXE	Preboot Execution Environment: rozruch komputera z sieci
RHEL	Red Hat Enterprise Linux: komercyjna dystrybucja Linuksa
SCCM	System Center Configuration Manager: dziś Configuration Manager, lokalne zarządzanie flotą

Skrót	Co znaczy
SMB	Server Message Block: protokół udziałów plików i drukarek Windows
SSE4.2	Streaming SIMD Extensions 4.2: zestaw instrukcji procesora wymagany od 24H2
SSO	Single Sign-On: jedno logowanie do wielu usług
TPM	Trusted Platform Module: układ przechowujący klucze i pomiary rozruchu
UEFI	Unified Extensible Firmware Interface: współczesny firmware płyty głównej
VBS	Virtualization-Based Security: izolowany hipernadzorcą obszar pamięci Windows
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
WDS	Windows Deployment Services: rola serwera do instalacji Windows przez sieć
WinPE	Windows Preinstallation Environment: minimalny Windows do instalacji i napraw
WinRE	Windows Recovery Environment: środowisko odzyskiwania Windows
WinRM	Windows Remote Management: zdalne zarządzanie Windowsem, podstawa PowerShell Remoting
WMIC	WMI Command-line: stare narzędzie wiersza poleceń do WMI
WSL	Windows Subsystem for Linux: podsystem uruchamiający Linuksa w Windows
WSUS	Windows Server Update Services: lokalny serwer zatwierdzania i dystrybucji aktualizacji

Fiszka

TYLKO ODCZYT

Wersja, kompilacja i edycja systemu na maszynie

```
# polecenie pomocnicze; nazwy wartości z dokumentacji Microsoftu
Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion' |
    Select-Object EditionID, DisplayVersion, CurrentBuild, UBR
```

Od tego zaczynamy każdą decyzję z tej listy: wydanie (`DisplayVersion`) mówi, ile zostało wsparcia, kompilacja (`CurrentBuild`) odróżnia linie serwisowe, a edycja (`EditionID`) — co w ogóle da się włączyć. Kompilacje: `26100` to 24H2, `26200` to 25H2, `22631` to 23H2, a `28000` to 26H1 — osobna linia, której nie da się podnieść do kolejnej rocznej aktualizacji funkcji.

Przykład (wynik ilustracyjny, nie z dokumentacji):

```
EditionID      : Professional
DisplayVersion : 24H2
CurrentBuild   : 26100
UBR            : 9550
```

□□ TYLKO ODCZYT

Sposób przyłączenia urządzenia: dsregcmd /status

```
# polecenie pomocnicze
dsregcmd /status | Select-String 'AzureAdJoined', 'DomainJoined', 'EnterpriseJoined'
```

Urządzenie hybrydowe ma jednocześnie `DomainJoined : YES` i `AzureAdJoined : YES`. Ta jedna informacja wyznacza trzy decyzje z dalszej części strony: który Autopilot (klasyczny czy device preparation), gdzie Windows LAPS trzyma hasło (AD albo Entra ID, nigdy oba) i czy zadziała przywracanie ustawień w OOBE (tylko Entra joined).

Przykład (wynik ilustracyjny, nie z dokumentacji):

```
             AzureAdJoined : YES
          EnterpriseJoined : NO
              DomainJoined : YES
```

□□ **AD** = Active Directory: katalog kont, komputerów i zasad w domenie Windows · **LAPS** = Local Administrator Password Solution: automatyczna rotacja haseł lokalnych administratorów · **OOBE** = Out-of-Box Experience: kreator pierwszego uruchomienia Windows

□□ TYLKO ODCZYT

Które zasady grupy faktycznie trafiają na maszynę: gpresult

```
# polecenie pomocnicze
gpresult /scope computer /r
```

Przed przejściem na Intune sprawdzamy, jakie GPO obejmują maszynę — zwłaszcza GPO Windows Update i bazy bezpieczeństwa. Maszyna hybrydowa objęta jednocześnie GPO Windows Update i profilem Intune dostaje dwa źródła prawdy; ustawienie `ControlPolicyConflict/MDMWinsOverGP` rozstrzyga konflikt tylko dla części polityk. Pełny raport w HTML daje `gpresult /scope computer /h raport.html`.

◫ **GPO** = Group Policy Object: obiekt zasad grupy w Active Directory · **HTML** = HyperText Markup Language: język stron WWW

◫ TYLKO ODCZYT

Inwentaryzacja całej floty naraz przez WinRM

```
# polecenie pomocnicze; nazwy wartości z dokumentacji Microsoftu
$komputery = Get-Content .\komputery.txt
Invoke-Command -ComputerName $komputery -ScriptBlock {
    Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion' |
        Select-Object EditionID, DisplayVersion, CurrentBuild, UBR
} -Credential (Get-Credential) |
    Select-Object PSComputerName, EditionID, DisplayVersion, CurrentBuild, UBR |
    Export-Csv .\inwentaryzacja-w11.csv -NoTypeInformation -Encoding UTF8
```

Ta sama kwerenda co w pierwszej karcie, uruchomiona równolegle na liście maszyn — wynik trafia do CSV, z którego od razu widać maszyny 24H2 w edycji Pro (termin 13 października 2026), 23H2 w Enterprise i Education (10 listopada 2026) oraz urządzenia 26H1. Wymaga działającego WinRM na maszynach docelowych — konfigurację opisuje strona WinRM — zarządzanie zdalne.

◫ **CSV** = Comma-Separated Values: tabela w pliku tekstowym, kolumny rozdzielone przecinkami · **WinRM** = Windows Remote Management: zdalne zarządzanie Windowsem, podstawa PowerShell Remoting

Mapa: co się zmieniło i gdzie to robimy

Temat	Co się zmieniło (2024–2026)	Gdzie się to ustawia	Wykonanie
Aktualizacje	„Windows Update for Business” to od 1 IV 2025 **polityki klienta Windows Update**; Autopatch od IV 2025 w Business Premium, A3+, E3+, F3; hotpatch domyślnie włączony od V 2026	GPO: Składniki systemu Windows → Windows Update; Intune: Update rings, Feature update policy, Autopatch	Hotpatch i Autopatch

Temat	Co się zmieniło (2024–2026)	Gdzie się to ustawia	Wykonanie
Secure Boot	wygasają trzy certyfikaty z 2011 roku: 24 VI, 27 VI i **19 X 2026**	rejestr, GPO (ADMX 25H2 v2.0), Intune Settings Catalog	Secure Boot: wymiana certyfikatów 2011 → 2023
Machine Identity Isolation	po KB5124008 (8 IX 2026) część maszyn traci relację zaufania z domeną	GPO Device Guard, Intune, rejestr	Machine Identity Isolation po KB5124008
Hasło lokalnego administratora	Windows LAPS wbudowany od 11 IV 2023; stary LAPS (MSI) zablokowany na 23H2+	GPO System\LAPS, CSP LAPS	Windows LAPS
Bezpieczeństwo domyślne	podpisywanie SMB od 24H2, plan wyłączenia NTLM, LSA protection, usunięte WMIC, PowerShell 2.0, WordPad; druk IPP od 1 VII 2026	GPO zabezpieczeń, rejestr, serwer druku	Bezpieczeństwo domyślne 24H2/25H2
Odporność i AI	Quick Machine Recovery domyślnie wyłączony w domenie; Recall domyślnie usunięty, Click to Do domyślnie włączony na urządzeniach zarządzanych	Recovery CSP, CSP WindowsAI, GPO Windows AI	Quick Machine Recovery, Recall i Click to Do
Lokalne źródło aktualizacji	WSUS przestarzały (IX 2024), ale działa; Microsoft Connected Cache ogólnie dostępny od VII 2025	portal Azure, host Ubuntu, RHEL 8/9 albo Windows przez WSL 2	Hotpatch i Autopatch · WSUS — czyszczenie i utrzymanie
Przygotowanie urządzeń	dwa równoległe produkty: Autopilot klasyczny i Autopilot device preparation	Intune	ta strona, sekcja „Jak to działa”
Uprawnienia administratora	Administrator Protection dostępne od KB5120998, domyślnie wyłączone	Intune Settings Catalog → Local Policies Security Options	ta strona, sekcja „Jak to działa”
Kopia ustawień użytkownika	Windows Backup for Organizations; od 26H2 kopia domyślnie włączona	Intune Administrative Templates, GPO	ta strona, sekcja „Jak to działa”

Kalendarz: terminy, które są twarde

Data	Co się dzieje	Co robimy

24 VI i 27 VI 2026 (minęły)	wygasły Microsoft Corporation KEK CA 2011 i Microsoft UEFI CA 2011	inwentaryzacja stanu certyfikatów — Secure Boot
od V 2026	hotpatch domyślnie włączony w Autopatch (ustawienie tenantowe, domyślnie Allow)	świadoma decyzja o ustawieniu tenantowym — Hotpatch i Autopatch
od 1 VII 2026	ranking sterowników drukarek zawsze preferuje wbudowany sterownik klasy IPP	przegląd kolejek wydruku — Bezpieczeństwo domyślne
8 IX / 18 IX 2026	KB5124008 i zerwane relacje zaufania; obejście potwierdzone przez Microsoft	sprawdzenie `MachineIdentityIsolation` — Machine Identity Isolation
13 X 2026	koniec aktualizacji 24H2 w edycjach Home i Pro	przejście na 25H2 (pakiet włączający, jeden restart)
14 X 2026	zaczyna się drugi rok komercyjnego ESU dla Windows 10	decyzja o ESU dla pozostałych maszyn z Windows 10 — wejście kosztuje od tego dnia 183 USD za urządzenie
19 X 2026	wygasa Microsoft Windows Production PCA 2011	pilotaż i wdrożenie nowych certyfikatów — Secure Boot
10 XI 2026	koniec aktualizacji 23H2 w edycjach Enterprise i Education	przejście na 25H2 — z 23H2 to pełna aktualizacja, nie pakiet włączający
1 VII 2027	koniec aktualizacji sterowników drukarek firm trzecich poza poprawkami bezpieczeństwa	docelowo sterownik klasy IPP albo Print Support Apps
12 X 2027 / 10 X 2028	koniec aktualizacji 25H2 (Home/Pro / Enterprise/Education)	—

> **Wydanie przez ISO to nie pakiet włączający.** Z 24H2 i 25H2 wydanie 26H2 przychodzi przez Windows Update jako pakiet włączający (ok. 174 KB, jeden restart), z 23H2 i starszych — jako pełna aktualizacja (ok. 6,5 GB). Instalacja 26H2 z nośnika ISO, np. przez `setup.exe` z SCCM albo MDT, to zawsze **pełna aktualizacja w miejscu**. Na 27 IX 2026 wydanie 26H2 jest w kanale Release Preview i nie ma daty ogólnej dostępności ani opublikowanych dat końca wsparcia.

Po co to istnieje

Klasyczny model zarządzania — Active Directory, zasady grupy, WSUS, SCCM — nie zniknął, ale domyślnym modelem nowych wdrożeń Windows 11 jest zarządzanie przez chmurę: tożsamość w Microsoft Entra ID, polityki w Microsoft Intune, dostarczanie urządzeń przez Windows Autopilot. Przejście nie jest wymianą jednego narzędzia na drugie, tylko rozdzieleniem ról, które w domenie pełniło jedno miejsce:

Wymiar	Zasady grupy (GPO)	Intune
Zasięg	tylko w sieci firmowej albo przez VPN	przez internet, wszędzie
Częstotliwość	przy logowaniu i co ok. 90 minut	cykl własny, niezależny od sieci firmowej
Mechanika	ustawienia dziedziczone przez strukturę jednostek organizacyjnych	CSP — ten sam interfejs, którym zarządza się telefonami
Kompletność	pełna	przez lata tylko część tego, co GPO; luka zmalała dzięki Settings Catalog i ADMX ingestion, ale nie zniknęła
Nowe funkcje 2024–2026	część (Secure Boot ma szablony ADMX, hotpatch nie)	wyłącznie albo przede wszystkim tu: hotpatch, Backup for Organizations, device preparation, raporty Autopatch
Koszt	w cenie Windows Server i licencji dostępowych	abonament na użytkownika

Jak to działa

Wydanie jako data ważności

Kadencja jest stała: jedna aktualizacja funkcji rocznie, w drugiej połowie roku; 24 miesiące wsparcia dla Home, Pro, Pro for Workstations i Pro Education, 36 miesięcy dla Enterprise, Education i IoT Enterprise; poprawki zbiorcze w drugi wtorek miesiąca. Wydania 25H2 i 26H2 to pakiety włączające nad wspólnym kodem 24H2 — różnią się tym, które funkcje są „włączone”, a w praktyce **resetują licznik wsparcia**. Same funkcje przychodzą w comiesięcznych aktualizacjach i są rozdawane stopniowo (CFR), niezależnie od numeru wersji — dlatego instalacja konkretnej KB nie gwarantuje, że nowa opcja od razu się pokaże.

Wyjątkiem jest **26H1** (kompilacja 28000, 10 II 2026): wydanie dostępne wyłącznie preinstalowane na wybranych nowych urządzeniach, na IX 2026 ze Snapdragonem X2, niedostępne przez Windows Update. Microsoft zaleca firmom pozostanie przy 24H2 i 25H2. Urządzenia z 26H1 nie mogą zaktualizować się do 26H2, bo bazują na innym rdzeniu Windows, i nie obsługują hotpatch. Nowy laptop ze Snapdragonem X2 kupiony w 2026 roku wydzielamy więc do osobnej grupy — pierścienie z docelową wersją 25H2 albo 26H2 go nie „podniosą”, a przed zakupem sprawdzamy listę agentów z komponentem jądra (EDR, VPN, DLP, sterowniki druku), bo emulacja Prism działa tylko w trybie użytkownika i nie obsługuje sterowników.

Autopilot i Autopilot device preparation

To dwa równoległe produkty, nie dwie wersje jednego:

Cecha	Device preparation	Autopilot klasyczny
Typ przyłączenia	**tylko Entra join**	Entra join **i Entra hybrid join**
Pre-provisioning / self-deploying (kiosk)	nie / nie	tak / tak
Rejestracja skrótu sprzętowego	niewymagana	wymagana
Strona stanu rejestracji (ESP)	tylko urządzeniowa, w OOBE	urządzeniowa i użytkownika
Systemy	Windows 11 24H2+ (22H2 i 23H2 z KB5035942)	Windows 10 i 11
Aplikacje / skrypty PowerShell w trakcie	do 25 „niezbędnych” / do 10	do 100 / ponad 10
Win32 i LOB w jednym wdrożeniu	tak	nie
Raportowanie	prawie w czasie rzeczywistym	nie w czasie rzeczywistym
Chmury rządowe (GCCH, DoD)	tak	nie

Device preparation ma od 2026 roku Enrollment Time Grouping (urządzenie trafia do grupy zabezpieczeń już przy rejestracji), Device association i Corporate identifiers; według omówienia KB5124008 powiązanie urządzeń jest ogólnie dostępne. **Jeśli nowe maszyny mają zostać hybrydowo przyłączone** — bo wymagają tego GPO, udziały, aplikacje z uwierzytelnianiem Kerberos bez Cloud Kerberos Trust — jedynym Autopilotem jest klasyczny, z Intune Connector for AD i zazwyczaj z VPN albo linią wzroku do kontrolera domeny. Device preparation to decyzja „nowe maszyny już nie w domenie”. Daty końca wsparcia klasycznego Autopilota ani hybrydowego przyłączenia w nim nie ogłoszono.

Administrator Protection

Użytkownik z grupy Administratorzy działa bez uprawnień, a przy operacji administracyjnej system tworzy token w ukrytym, generowanym przez system, profilowo odseparowanym koncie, po czym token jest niszczony; autoryzacja przez Windows Hello, bez automatycznych podniesień. Dostępne od KB5120998 (27 VIII 2026), **domyślnie wyłączone**, wymaga restartu; edycje Home, Pro, Enterprise i Education, nie Windows 365, hosty sesji AVD ani Windows Server. Microsoft zastrzega, że funkcja „nie jest formalną granicą bezpieczeństwa”.

Włączenie w Intune: Settings Catalog → Local Policies Security Options → „User Account Control Type Of Admin Approval Mode” oraz „User Account Control Behavior Of the Elevation Prompt for Administrator Protection” (CSP `UserAccountControl_TypeOfAdminApprovalMode` i `UserAccountControl_BehaviorOfTheElevationPromptForAdministratorProtection`). Pilotaż jest obowiązkowy, bo lista niezgodności jest długa: nie włączamy na Cloud PC, AVD i urządzeniach potrzebujących Hyper-V lub WSL; w sesjach podniesionych nie ma SSO, **dyski sieciowe są niedostępne z aplikacji podniesionych**, ustawienia nie przechodzą między profilami, po instalacji podniesionej brakuje ikon w Start, a profile mobilne są niezgodne. Na stanowiskach deweloperskich z WSL i Hyper-V raczej nie; dla floty z lokalnymi administratorami to alternatywa

dla płatnego EPM.

Windows Backup for Organizations

Kopia **ustawień i preferencji użytkownika oraz listy aplikacji ze Sklepu** — nie plików — co 8 dni zadaniem harmonogramu albo ręcznie; przywracanie w OOBE po zalogowaniu tym samym kontem Entra. Kopia wymaga urządzenia Entra joined albo Entra hybrid joined, przywracanie — Windows 11 22H2 w kompilacji 22621.3958 lub nowszej i urządzenia **Entra joined**; przy Autopilot tylko tryb user-driven. Polityki: w Intune Administrative Templates\Windows Components\Sync your settings → „Enable Windows Backup”; przywracanie — polityka rejestracji dla tenanta albo „Windows Backup And Restore → Enable Windows Restore”. Konfigurujemy **albo przez GPO, albo przez CSP**, nie mieszanką. Dostęp warunkowy potrafi blokować przywracanie — potrzebny jest wyjątek dla aplikacji o ID `d32c68ad-72d2-4acb-a0c7-46bb2cf93873`. Od VII 2026 zarządzanie Enterprise State Roaming przeniesiono do tej funkcji, a od 26H2 kopia jest domyślnie włączona na kwalifikujących się urządzeniach.

> Nie wyłączamy `EnableActivityFeed`, `PublishUserActivities`, `UploadUserActivities`, `EnableCDP` ani `AllowConnectedDevices` — inaczej kopia po cichu się nie wykona. Wiele baz bezpieczeństwa, w tym CIS, wyłącza właśnie Activity Feed i CDP.

Windows 365 i Windows 365 Link

Windows 365 to osobisty pecet z Windows w Azure za stałą stawkę miesięczną na użytkownika. Cloud PC dostaje ESU bez dopłaty, a fizyczny komputer z Windows 10 łączący się z Cloud PC — do trzech lat ESU. Windows 365 Link to terminal bez lokalnych danych, bez lokalnych aplikacji i **bez lokalnego użytkownika z prawami administratora**, zarządzany wyłącznie przez Intune (TPM 2.0, Secure Boot, VBS, HVCI, BitLocker, Application Control, czujnik Defender EDR). Administrator Protection nie obsługuje Cloud PC; certyfikaty Secure Boot na Cloud PC mają własną stronę Microsoftu, a na maszynach Trusted Launch (także Cloud PC i AVD) występuje znany problem ze zdarzeniem 1795 przy aktualizacji KEK — według Microsoftu „bez natychmiastowej akcji klienta”.

ESU dla pozostałych maszyn z Windows 10

Cennik komercyjny za urządzenie: rok 1 — 61 USD, rok 2 (od 14 X 2026) — 122 USD, rok 3 — 244 USD; kupuje się tylko pełne lata, a kupując rok 2, trzeba zapłacić też rok 1 — stąd **183 USD za urządzenie** dla firmy, która wchodzi dopiero teraz. Aktywacja kluczem MAK z Microsoft 365 admin center albo przez Intune, tylko Windows 10 22H2. Bez dopłaty w AVD, maszynach wirtualnych

Azure, Windows 365, Azure Local, Azure Dedicated Host i Azure VMware Solution. Darmowe ESU w EOG dotyczy wyłącznie konsumentów — firmy w Polsce płacą jak wszędzie. Rabatu dla urządzeń zarządzanych z chmury strona Microsoftu nie wymienia.

Lista czynności na IV kwartał 2026

> Wybór i kolejność czynności są syntezą autora, a nie zaleceniem Microsoftu; fakty, na których się opierają, są na stronach, do których prowadzą odnośniki. Lista zakłada flotę Windows 11 w domenie AD z GPO, przed wdrożeniem Intune i Entra ID.

Pilne — przed 13, 19 października i 10 listopada 2026

1. **Machine Identity Isolation — dziś.** Odczyt `MachineIdentityIsolation` na próbce maszyn i w politykach; przy kontrolerach poniżej poziomu funkcjonalnego 2025 wartość 0; procedura naprawy kanału i hasło LAPS pod ręką — Machine Identity Isolation po KB5124008.
2. **24H2 Home/Pro → 25H2 przed 13 października 2026** (docelowa wersja w GPO albo Feature update policy); maszyny 23H2 dostaną pełną aktualizację; Enterprise/Education na 23H2 — przed 10 listopada 2026.
3. **Secure Boot — inwentaryzacja** `UEFICA2023Status` i zdarzeń 1808/1801/1803, **pilotaż** na co najmniej 4 maszynach na kombinację producent/model/BIOS, klucze BitLocker dostępne, PXE za dyskiem — Secure Boot: wymiana certyfikatów.
4. **Nośniki serwisowe** (WinPE, pendrive'y, obrazy WDS/PXE) odtworzone po przejściu na boot manager podpisany Windows UEFI CA 2023, zanim ktokolwiek odwoła PCA 2011 w DBX.
5. **Hyper-V** — hosty i goście z aktualizacjami co najmniej z 10 III 2026 (Server 2025 — z 14 IV 2026).
6. **Hosty linuksowe z Secure Boot** — najpierw zmienne UEFI, potem shim; wytyczne dystrybucji, w tym Red Hat.
7. **ESU** dla pozostałych maszyn z Windows 10 — decyzja przed 14 października 2026.

Planowanie Intune

8. **Hybrid join czy Entra join** dla nowych maszyn — wyznacza Autopilot, miejsce kopii hasła LAPS i przywracanie w OOBE (sekcja „Jak to działa” wyżej).

9. **Współzarządzanie**: obciążenia „Windows Update policies” i „Device configuration” na Intune; usunięcie równoległych GPO Windows Update — Hotpatch i Autopatch.
10. **Licencje i edycja** pod Autopatch i hotpatch; świadome ustawienie tenantowe „Hotpatch” — Hotpatch i Autopatch.
11. **Pierścienie** nawet w firmie na trzydzieści maszyn: pilotaż, grupa właściwa, grupa krytyczna z maksymalnym odroczeniem.
12. **Delivery Optimization i Connected Cache** jako lokalne źródło bajtów zamiast WSUS; WSUS zostawiamy, dopóki działa.
13. **Windows LAPS** — migracja ze starego MSI — Windows LAPS.
14. **Quick Machine Recovery** — włączenie przez Recovery CSP, sprawdzenie WinRE — Quick Machine Recovery, Recall i Click to Do.
15. **Windows Backup for Organizations** — bez wyłączania Activity Feed i CDP, wyjątek dostępu warunkowego, decyzja o domyślnej kopii w 26H2.
16. **Arm (Snapdragon X2)** — osobna grupa: 26H1, brak ścieżki do 26H2, brak hotpatch, lista agentów z komponentem jądra.

Utwardzanie — praca ciągła

17. **NTLM** — audyt teraz; **SMB** — lista urządzeń z dostępem gościa albo bez podpisywania; **LSA protection** na maszynach zaktualizowanych z Windows 10 — Bezpieczeństwo domyślne 24H2/25H2.
18. **Skrypty** `.vbs` w skryptach logowania GPO i wywołania `wmic` przepisane na PowerShell 5.1/7.x i `Get-CimInstance`.
19. **Drukarki** — które kolejki po 1 lipca 2026 wybrały sterownik klasy IPP.
20. **Administrator Protection** — pilotaż na stanowiskach bez WSL, Hyper-V i intensywnie używanych dysków sieciowych.
21. **Recall i Click to Do** — świadoma decyzja; Click to Do jest w firmach domyślnie włączony — Quick Machine Recovery, Recall i Click to Do.
22. **DirectAccess**, jeśli jeszcze gdzieś jest — przestarzały od VI 2024; Microsoft zaleca Always On VPN.

Decyzje stałe

- **Pierwsza decyzja jest licencyjna, nie techniczna.** Home w organizacji nie ma sensu — nie da się odroczyć aktualizacji, nie ma zasad grupy ani zarządzanego BitLockera, jest wymuszone konto Microsoft. Pro to minimum; Enterprise kupuje się dla LTSC, najniższego poziomu telemetrii, a od 2025 roku także dla hotpatch.
- **LTSC** rozwiązuje realne problemy — stabilność, brak reklam, przewidywalność — i jest dostępny wyłącznie w licencjonowaniu zbiorowym.

- **Kopie zapasowe niezależne od OneDrive.** Przy aktualizacji funkcji traktujemy maszynę jak taką, która może nie wrócić.
- **Inwentaryzacja zgodności**: TPM 2.0 włączony w firmware (najczęstsza przyczyna fałszywego „niezgodny”), UEFI zdolny do Secure Boot, dysk w GPT (konwersja `mbr2gpt`), procesor z listy; maszyna z obejściem wymagań i bez SSE4.2 nie uruchomi 24H2 w ogóle.
- **Konta lokalne w OOBE** — w organizacji rozwiązaniem jest domena, Entra ID, Autopilot albo nośnik z `autounattend.xml`, przetestowany na bieżącej kompilacji.

Analogia

Zasady grupy działają jak tablica ogłoszeń na korytarzu biura: każdy, kto przyjdzie do budynku, przeczyta aktualną wersję, a kto pracuje z domu, nie dowie się o zmianie, dopóki nie wejdzie przez drzwi — albo przez tunel VPN. Intune działa jak komunikat wysłany na służbowy telefon: dociera wszędzie, gdzie jest internet. Ograniczenie analogii: tablica ogłoszeń przez dwadzieścia lat obrosła w tysiące szczegółowych przepisów, a komunikaty na telefon wciąż nie mają odpowiednika każdego z nich — dlatego przez okres przejściowy trzeba pilnować, żeby ta sama sprawa nie była ogłaszana w obu miejscach naraz, w dwóch różnych brzmieniach.

Częste błędy

Dwa źródła prawdy dla Windows Update. Maszyna hybrydowa z GPO Windows Update i profilem Intune jednocześnie — przy współzarządzaniu obciążenie „Windows Update policies” musi być przełączone na Intune, inaczej strony się nadpisują.

Liczenie na to, że Pro „ma wszystko, co jest w Intune”. Polityki Secure Boot z Intune były na Pro blokowane błędem 65000 przez usługę licencyjną; hotpatch według prasy działa tylko na Enterprise i Education. Edycja Pro w MDM bywa obywatelem drugiej kategorii.

Baza bezpieczeństwa wdrożona w całości, bez czytania. Wyłączone Activity Feed i CDP po cichu wyłączają Windows Backup for Organizations, a wartość Enforcement dla Machine Identity Isolation z bazy przez rok nie robiła nic, dopóki KB5124008 nie kazała jej respektować.

Traktowanie laptopa ze Snapdragonem X2 jak reszty floty. 26H1 to inna linia serwisowa — bez ścieżki do 26H2 i bez hotpatch.

□□ Ćwiczenia

>

> Ćwiczenia wymagają dostępu administratora do kilku maszyn z Windows 11 w domenie i działającego WinRM.

Ćwiczenie 1 — mapa własnej floty

```
# polecenie pomocnicze; nazwy wartości z dokumentacji Microsoftu
Import-Csv .\inwentaryzacja-w11.csv |
    Group-Object DisplayVersion, EditionID |
    Select-Object Count, Name |
    Sort-Object Count -Descending
```

Na podstawie CSV z czwartej karty grupujemy maszyny według wydania i edycji. Które grupy mają twardy termin w tym kwartale?

Odpowiedź

Maszyny z `DisplayVersion` 24H2 i `EditionID` Core (Home; także CoreN i CoreSingleLanguage — nazwy SKU z dokumentacji Intune for Education) albo Professional tracą aktualizacje 13 października 2026; maszyny 23H2 w edycjach Enterprise i Education — 10 listopada 2026. Pierwsze przechodzą na 25H2 pakietem włączającym (jeden restart), drugie pełną aktualizacją. Jeśli w CSV pojawi się kompilacja 28000, to jest 26H1 — osobna grupa, której pierścienie z docelową wersją 25H2 nie obejmą.

Pytania kontrolne

1. Firma chce, żeby nowe laptopy nadal dostawały GPO z domeny. Który Autopilot wybiera i dlaczego?

Odpowiedź

Autopilot device preparation obsługuje wyłącznie Entra join. Klasyczny Autopilot obsługuje też Entra hybrid join, więc tylko on pozwala nowemu urządzeniu zostać w domenie. Wybór device preparation oznacza w praktyce decyzję, że nowe maszyny nie są już w domenie — ze skutkami dla GPO, udziałów i aplikacji z Kerberosem.

2. Czy urządzenie hybrydowe może trzymać hasło LAPS jednocześnie w AD i w Entra ID?

Odpowiedź

Nie. Hasło z Windows LAPS trafia na urządzeniu hybrydowym albo do AD, albo do Entra ID — nigdy do obu; wybór jest jednorazowy dla urządzenia i trzeba go podjąć razem z decyzją o przyłączeniu.

3. Dlaczego ESU kupione 15 października 2026 kosztuje 183 USD za urządzenie, a nie 122?

Odpowiedź

Firma, która nie kupiła roku 1, a wchodzi w roku 2, płaci za oba lata: 61 USD za rok, który już minął, i 122 USD za rok bieżący — razem 183 USD za urządzenie. ESU kupuje się wyłącznie w pełnych latach.

Powiązane: Hotpatch i Autopatch · Secure Boot: wymiana certyfikatów 2011 → 2023 · Machine Identity Isolation po KB5124008 · Windows LAPS · Bezpieczeństwo domyślne 24H2/25H2 · Quick Machine Recovery, Recall i Click to Do · WinRM — zarządzanie zdalne · WSUS — czyszczenie i utrzymanie

Źródła: Windows 11 release information · Windows 11, version 26H1 · Autopilot device preparation — porównanie · Administrator protection · Windows Backup for Organizations · Windows 365 Link · Extended Security Updates · Windows Central — 26H2 z ISO · emulacja x86 na Arm (Prism) · strona serii *Windows 11* (kontekst i historia)

Revision #2
Created 2026-09-27 17:44:13 UTC by Tomasz Konieczny
Updated 2026-09-27 17:44:25 UTC by Tomasz Konieczny