CloudBoostUP

Patching Compliance Migration

Move off retired Azure Automation Update Management onto Azure Update Manager, with audit trail and per-BU accountability built in

WHAT WE HEARD FROM A PLATFORM LEADER AT A FORTUNE-100 PHARMA

"going back to enforcing certain things like vm patching because of tenants just not doing it and the risks attached to it"

Why this. Why now.

Microsoft retired Azure Automation Update Management on 31 August 2024. Orgs still running the legacy stack are on borrowed time: schedules and assessment work today, but the platform underneath is deprecated, security investments have stopped, and the migration tool is the documented path forward.

The phrase "tenants just not doing it" usually decodes to three patterns: subs provisioned outside the central onboarding flow that never got patching; reboot setting fixed to Never so patches install but never take effect; opt-outs in email with no expiry and no audit trail. The fix is a platform contract: opt-out as a queryable Azure resource with TTL, per-BU dashboards exported weekly, cost-allocation pressure when exceptions persist.

What you get in 6 weeks

Migration runbook + drop-in IaC	Replacement onboarding pipeline preserving your existing wave tag contract (Wave1 / Wave2 / Wave3). Drops in for the legacy Function App or Automation Account orchestration. PR-ready in week 2.
Azure Update Manager + Maintenance Configurations	Dynamic Scoping that evaluates tags at run time so new VMs auto-enroll. Reboot setting moves from Never to IfRequired with platform-defined window reservations. Full classification coverage Windows and Linux.
Azure Policy at scale	Required maintenance config + periodic assessment. Slots into your existing auto-remediation initiative pattern. Per-management-group assignments via your existing scope conventions.
Opt-out registry as queryable resource	Storage Table backed by Logic App approval flow. Mandatory justification + TTL + expiry alerts. ServiceNow integration via existing webhook pattern. No more email-thread exceptions.
Per-BU compliance Workbook	Resource Graph KQL queries over patchassessmentresources + patchinstallationresources. Drill-down by BU tag. Weekly PDF export to BU CIO via existing SIEM forwarder pipe.
Cost-allocation overlay	Tag taxonomy + chargeback formula tied to vulnerability count. Compliance Manager mapping to NIS2, DORA, ISO 27001, GxP. Audit team gets one artifact instead of chasing email threads.

Who it is for

- Platform / Cloud Ops leads at 5,000-plus-employee regulated orgs running multi-tenant Azure estates.

- Orgs still running legacy Azure Automation Update Management or Update Management agent-based patching.
- Teams where patching opt-outs live in email and nobody can answer “who is non-compliant and why” in hours.
- Teams under audit pressure: NIS2, DORA, ISO 27001, GxP, 21 CFR Part 11, or sector-specific patch SLAs.

How it works

Week 1	Inventory baseline. Resource Graph audit of current patching state per management group. Wave-tag coverage. Subs that bypassed onboarding. Gap report with named owners.
Week 2	Drop-in replacement onboarding pipeline using Azure Update Manager + Maintenance Configurations + Dynamic Scoping. Preserves your wave contract. Reboot setting set to IfRequired.
Week 3	Azure Policy assignments at scale. Required maintenance config + periodic assessment. Slotted into your existing auto-remediation initiative. Per-management-group scope.
Week 4	Opt-out registry as Storage Table + Logic App approval workflow. BU CIO approval routing. ServiceNow integration through existing webhook. Mandatory TTL and expiry alerts.
Week 5	Per-BU compliance Workbook. Weekly PDF export Logic App. Compliance state mapped to your existing GRC pipe. Cost-allocation overlay deployed with your FinOps team.
Week 6	Migrate one wave end-to-end as the pattern proof. Lowest-risk wave chosen with your platform team. Remaining waves on your roadmap with our runbook. Handoff session (4 hours live + recorded).

What you leave with

Code + config

- ✓ Replacement onboarding pipeline (drop-in IaC + script)
- ✓ Azure Policy assignments + initiative integration
- ✓ Opt-out registry (Storage Table + Logic App)
- ✓ Workbook JSON + KQL query library

Documentation + runbooks

- ✓ Migration runbook (per-wave + per-management-group)
- ✓ Audit-response runbook (regulator question to answer in hours)
- ✓ Cost-allocation formula spec for your FinOps team
- ✓ Wiki documentation published in your ADO

What we do not do

We do not patch your VMs (your platform ops team operates the pattern). We do not validate patches in your test environments. We do not act as your exception approver (your BU CIOs own that decision). We do not replace your SIEM, GRC, or cloud security tools; we integrate with what your platform owns.

Adrian Komorek
Founder, CloudBoostUP • Platform engineering for regulated multi-tenant Azure estates
adrian.komorek@cloudboostup.com • +48 695 546 826
cloudboostup.com • linkedin.com/in/adriankomorek

Engagement model
Fixed scope • 6 weeks • EU rate band
Reference price on request