

IT SECURITY CHECKLIST

Third-Party Patching: Your Options Compared

Easy2Patch vs. native Intune/SCCM tooling vs. manual packaging — a side-by-side for IT decision-makers.

How the three approaches stack up

You already patch Microsoft apps. The question is how you'll cover the third-party gap – and what each path costs you in time and risk.

Criterion	Easy2Patch	Native Intune / SCCM	Manual packaging
Third-party app coverage	✓ 750+ apps maintained for you	✗ Limited; mostly Microsoft apps	~ Any app, but one at a time
Update packaging	✓ Automated, pre-tested packages	~ Manual import & wrapping	✗ Fully manual per version
Works inside Intune / SCCM	✓ Native to your existing console	✓ It is the console	~ Scripts bolted on
New agents required	✓ None – uses your infrastructure	~ None	✓ None
Time to patch a new CVE	✓ Hours – package is ready	~ Days – find, test, wrap	✗ Days to weeks, per app
Patch testing	✓ Pre-tested before release	✗ You test everything	✗ You test everything
Compliance reporting	✓ Built-in, per device & app	~ Basic Microsoft reporting	✗ Build your own
Engineering effort	✓ Low – set policy,	~ Medium – ongoing manual work	✗ High – constant repackaging
Scales across endpoints	✓ Thousands with one policy	~ Yes for MS apps only	✗ Effort grows with each app

Close the gap without adding work.

Easy2Patch patches 750+ third-party apps directly inside the Intune & SCCM

- ✓ Console You Already Run – Automated Packaging, Pre-Tested Updates, And
- ✓ Compliance Reporting Out Of The Box.
- ✓ No New Agents, No Parallel Tooling
- ✓ Patch New CVEs In Hours, Not Weeks
- ✓ Audit-Ready Compliance Reporting Included

Book A Free Demo