QUISITIVE

Follow the flow to find your

Ideal Patch Approach

Do you have to patch regularly? YES

Does ideal patch management look the same for everybody? NO

Poor patch management causes **60%** of breaches

Don't patch

Choose strategic, ongoing **patching support** with **comprehensive reporting**

Leverage outside **patching support as needed** with **basic reporting access**

Handle patching in-house

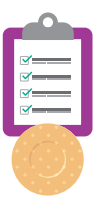
Your patching profile:

1. Don't patch

Bad idea. Even small companies with very little bandwidth and resources should make patching a priority. **60% of them go out of business** within six months of a cyber-attack.

2. Strategic, ongoing patching support with comprehensive reporting

To balance mission-critical tasks with innovative initiatives, and thus thrive in today's competitive digital era, organizations are having to get creative with IT management. IT Lifecycle Management services allow companies to funnel more energy and resources towards their business differentiators, while providing reliable support with reporting to prove it.



3. Patching support as-needed with basic reporting

While very few companies have the internal IT manpower to effectively handle patch management in-house, some may only need sliding-scale patching support. This option makes the most sense for organizations with moderate ambitions around digital innovation, lower-stake security and compliance demands, and an adequately staffed IT team.

4. In-house patching

This option will only be efficient and effective for a small majority: large, well-established companies with a robust IT team that includes members whose primary focus is patching.

Quisitive offers holistic patching support

Connect with an expert: **ask@quisitive.com**

QUISITIVE

quisitive.com