Software patching has for years been one of those tedious, and sometimes angst filled, processes that are simply part of the job. Just about every software company now issues patches and updates for their products in order to keep software secure and efficient. It is integral to the operation of software.

But patching, while necessary, is often a challenge for organizations because of the high volume of patches released daily and monthly. Some cloud vendors are recommending that rather than patching, organizations should instead fix the image and redeploy in order to update server instances. We reached out to IDG influencers to get their perspective on whether patching was dead or alive and how they think business should handle the process today.

“Software patching is both very much alive, and unlikely to meet its demise anytime soon. If anything, with software now handling more of our world than ever before, and more business value residing in data, the importance of software patching has never been greater.”

MICHAEL SKAFF (@mskaff)
CIO for Jewish Senior Living Group

Adam Stein thinks patching is an important part of IT operations that isn’t going away. “Software patching is alive and kicking to the tune of nearly $1 billion (USD) annually over the next four years,” he says. “This is due to most SaaS and on-premises software application vendors underspending on security, functional and UX testing, even with client’s increasing sensitivity to the costs of compliance breaches and confidential information theft.”

“This leaves a tremendous patch requirement gap in nearly every IT industry, including enterprise apps, IoT, and semiconductors,” he continues. “The recent Spectre semiconductor software vulnerability debacle shows that large gap. Essentially all major computer and mobile chips were affected by the Spectre flaw. Every chip customer, including consumer device manufacturers, will require a software patch to block this potent attack vector.”

ADAM STEIN (@apsteinz)
Principal at APS Marketing, Inc.
Securing Make Patching Essential

The recent Spectre flaw is a good example of the kind of risk-based issues that regularly prompt the need for patches to be pushed out and deployed quickly.

Who is Responsible?

It’s clear patching is essential to address flaws and keep software secure — but many noted the process to release and deploy patches is changing.

Security Makes Patching Essential

With cybercrime rising strongly and massive vulnerabilities being continuously found, software patching remains the best option to safeguard the integrity of our systems and, again, that involves business-critical applications, too.

Mike D. Kail would agree. “Implementing best practices around code and application hygiene is paramount to overall security.”

Software patching is not dead — as long as software is being written, it will need to be patched. However, where the patches are done and by whom may change. As more apps/software move to [the] cloud, the patches will be more invisible and automatic, and much more transparent to end users.

“Software patching in the traditional sense that vendors like Microsoft can release patches on a regular cadence [like] Patch Tuesday is dead,” says Conklin. “This doesn’t mean patching is dead, but that we cannot plan for periodic structured patch releases. There are too many third-party libraries and frameworks in software today to limit patching to a schedule that a vendor can control.”

“Software patching in the traditional sense that vendors like Microsoft can release patches on a regular cadence [like] Patch Tuesday is dead,” says Conklin. “This doesn’t mean patching is dead, but that we cannot plan for periodic structured patch releases. There are too many third-party libraries and frameworks in software today to limit patching to a schedule that a vendor can control.”

“Software patching in the traditional sense that vendors like Microsoft can release patches on a regular cadence [like] Patch Tuesday is dead,” says Conklin. “This doesn’t mean patching is dead, but that we cannot plan for periodic structured patch releases. There are too many third-party libraries and frameworks in software today to limit patching to a schedule that a vendor can control.”

“Software patching in the traditional sense that vendors like Microsoft can release patches on a regular cadence [like] Patch Tuesday is dead,” says Conklin. “This doesn’t mean patching is dead, but that we cannot plan for periodic structured patch releases. There are too many third-party libraries and frameworks in software today to limit patching to a schedule that a vendor can control.”

“Software patching in the traditional sense that vendors like Microsoft can release patches on a regular cadence [like] Patch Tuesday is dead,” says Conklin. “This doesn’t mean patching is dead, but that we cannot plan for periodic structured patch releases. There are too many third-party libraries and frameworks in software today to limit patching to a schedule that a vendor can control.”

“Software patching in the traditional sense that vendors like Microsoft can release patches on a regular cadence [like] Patch Tuesday is dead,” says Conklin. “This doesn’t mean patching is dead, but that we cannot plan for periodic structured patch releases. There are too many third-party libraries and frameworks in software today to limit patching to a schedule that a vendor can control.”

“At the end of the day, timely, automated patching means reduced risk of security exposure, a lower cost of managing servers, and faster response to immediate threats. For that reason, it’s clear that not only is software patching not dead, but timely software patching is more important than ever.