RECAST SOFTWARE

Reduce your Attack Footprint

by Automating Software Patching

The evolution of IT infrastructure and system management accelerated with the 2020 global pandemic, a decisive moment that etched Work from Home (WFH) and hybrid work into our public consciousness. Security Officers and IT Administrators now manage environments that must provide a smooth user experience for employees regardless of their location, while also maintaining an environment hardened against sophisticated threats. This maintenance requires staff training, the active management of hardware, and both operating system and third-party software management.

Kaspersky Labs* identified software vulnerabilities as the leading cause of the costliest breaches in 2021, outpacing phishing for the first time. This data means that organizations need to quickly update third-party software to improve their cybersecurity position and reduce risk. In addition to patching, IT teams must also manage the use of third-party applications, including user-installed apps. The **breach at LastPass**** in late 2022 painfully showcases the risks lurking within third-party applications. Reducing risk requires minimizing human error, automating when possible, and constant vigilance. Read on to better understand the tripping points for most companies, as well as best practices within the third-party patching space.

---

* Third party incidents became most costly enterprise data breaches in 2021 - Kaspersky

** LastPass Says DevOps Engineer Home Computer Hacked - SecurityWeek

The Dual Menace

Cybercriminals do not relent. Neither do the software updates that patch exploitable vulnerabilities. IT teams facing these dual challenges must remain agile and vigilant, which requires the professional help of an internal team or patching automation software.

First, what are the obstacles to understand and overcome?

A Broad Attack Surface

Every unpatched app or delayed update expands risk

Inefficient or flawed patching solutions and unknown third-party software in environments leave openings for intrusion. Cyberattack threats loom perpetually.

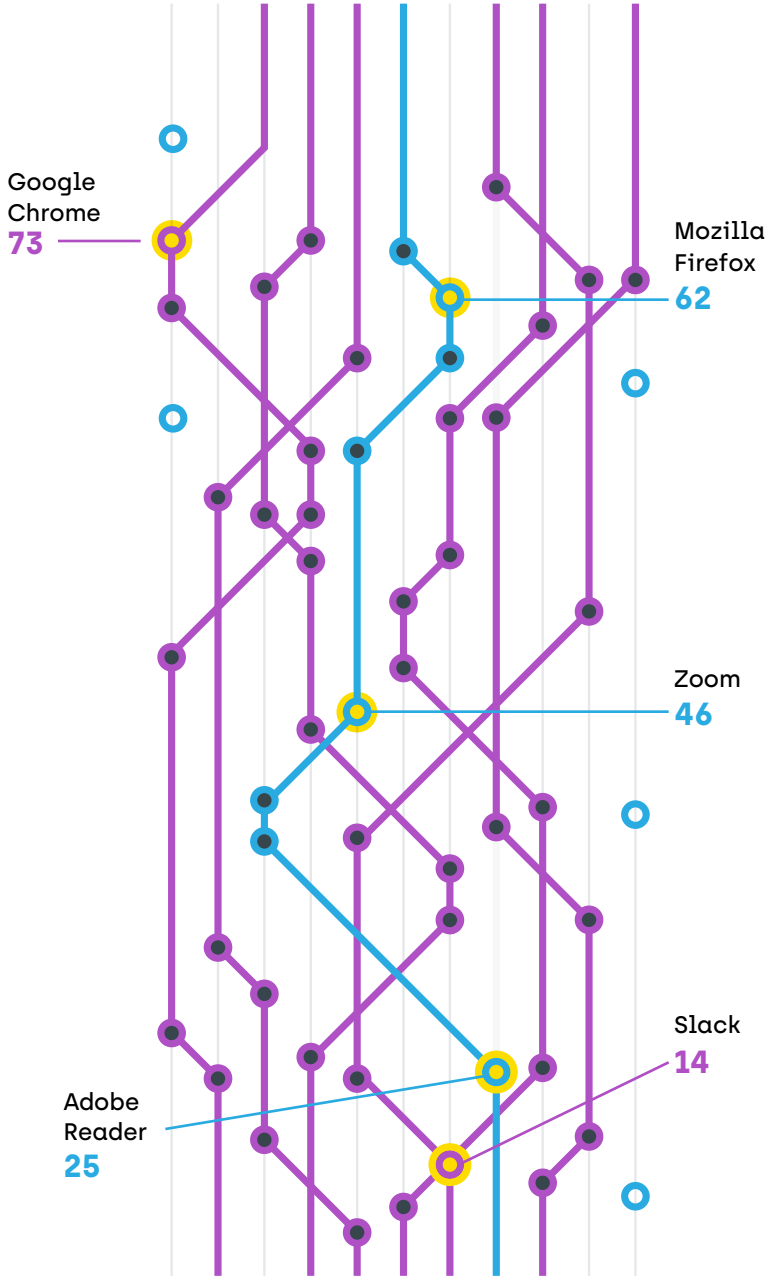
- In 2021, 93% of companies experienced a breach connected to third-party vendors.
- In 2022, the average cost of a breach globally was $9.4 million.*

* Cost of a data breach 2022 | IBM

"Nation state actors, much like ransomware and criminal operators, have responded to increased exposure by moving toward targeting poorly configured or unpatched enterprise systems (VPN/VPS infrastructure, on-premises servers, third-party software) to perform living-off-the-land attacks."**

- John Lambert, Corporate Vice President and Distinguished Engineer, Microsoft Threat Intelligence Center

** Microsoft Digital Defense Report 2022



Eternal Stream of Software Updates

Patching is unrelenting

Most companies operate with dozens, even hundreds of software titles in their stack. A single piece of vital software often requires five to ten updates every year.

2022 updates for common software titles:

- Adobe Reader - 25 patches
- Google Chrome – 73 patches
- Mozilla Firefox - 62 patches
- Slack – 14 patches
- Zoom – 46 patches

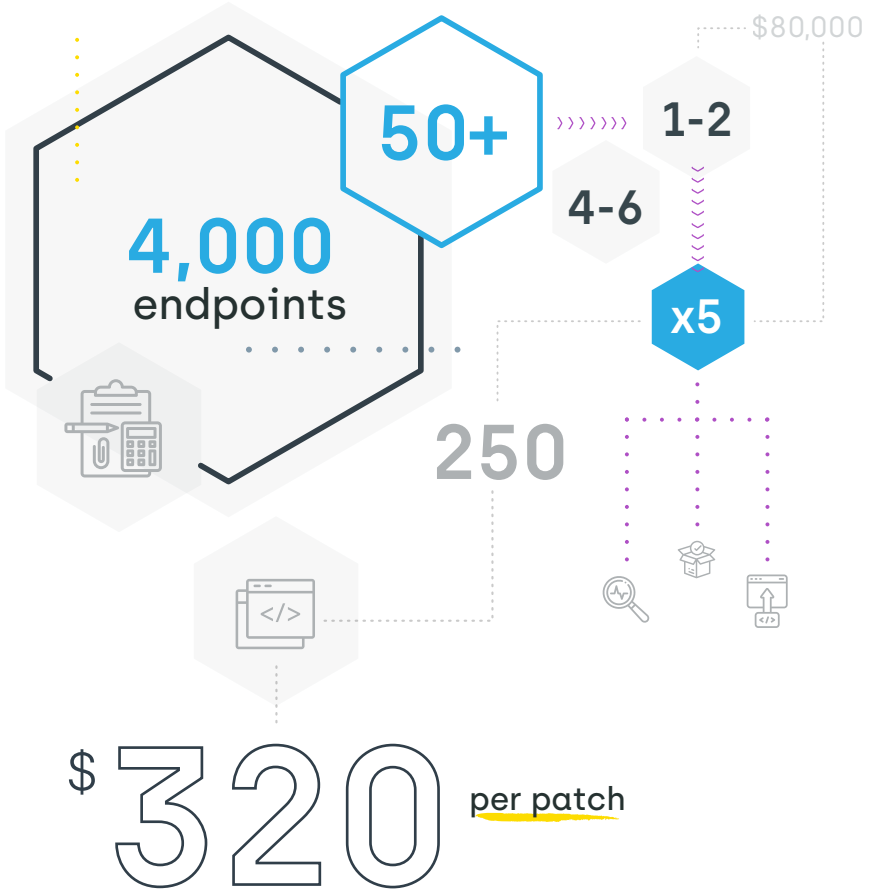
The multiplier effect of 5-10 patches overlayed with 50-100 software titles adds up to a significant job for an IT patching team.

Manual Patching Weaknesses

The labor of little love

In-house patching teams can take on the task of patch management. However, this strategy requires a significant number of hours and doesn't allow for weekends or holidays to interrupt the necessary vigilance. The reality is that in-house teams too often lead to patching delays, and therefore increased security vulnerabilities.

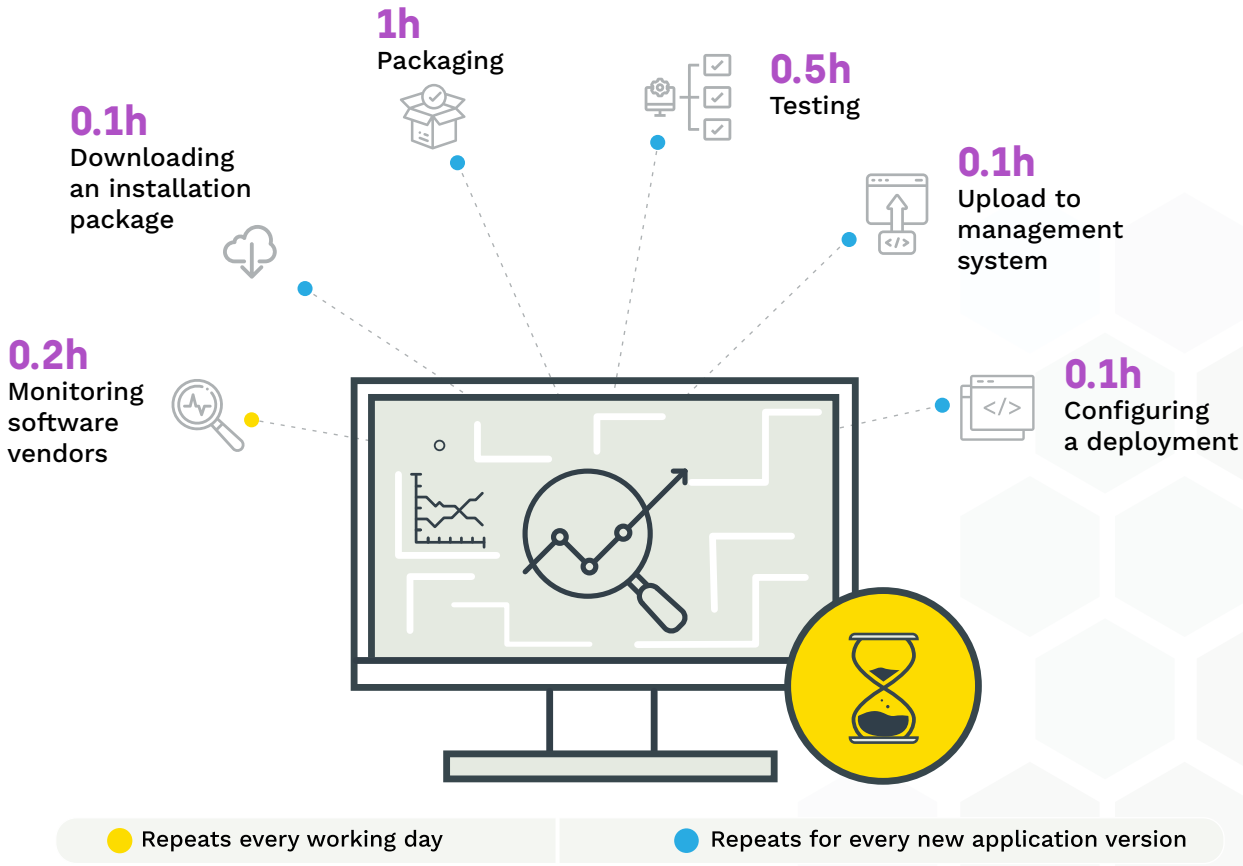
- A standard, hypothetical mid-size organization may have 4,000 endpoints in their environment with 50+ applications.
- This hypothetical company often has 4 to 6 people on the endpoint management team and 1 or 2 of them are responsible for the packaging and patching process.
- With an estimated 5 patches per title per year, the patching team will need to successfully test, package, and deploy 250 updates per year. This equates to $320 per patch.*



* Equation assumptions: 1 full-time patching employee with a total compensation package of $80,000 and 250 patches per year (50 titles with 5 patches each). $80,000 ÷ 250 = $320 per patch. These are conservative estimates.

The In-House Patching Process

The manual process is also unrelenting and time consuming: pilot, preproduction, production group test patches, and then the final company-wide patch push. It isn't uncommon to have a team readying the final company-wide patch launch only to see a new patch released by the software vendor only two or three days later. The current packaging process will need to be replicated again, before the first patch ever crosses the finish line.



It isn't uncommon to have a team readying the final company-wide patch launch only to see a new patch released by the software vendor only two or three days later.

No Rest or Holidays

Vulnerabilities don't pause for the holidays. Google Chrome, for instance, released a vital zero-day patch in 2022 the day after Thanksgiving in the United States. Is your patching team prepared to begin testing and packaging over holiday breaks and weekends?

Human Fallibility

Human error is a constant. In-house patching introduces human error into the process. This can lead to malfunctioning apps, user downtime, and expanded periods of threat exposure. For instance, when monitoring for new updates, patch teams can miss one. Teams can also make mistakes when defining deployments or by running a faulty test that misses a changed feature that is incompatible with your other apps' processes. Human error is an inevitability.

A survey of 200 business leaders cited "a reduction in manual errors" as the top reason for automating manual processes.*

* WorkMarket 2020 In(Sight) Report: What AI & Automation Really Mean for Work (pg. 13)

Custom, In-House Software Adds Complexity

A unique challenge

Some organizations utilize custom applications built for their specific environment. Managing updates for this custom software requires additional steps.

In-house software can be very vulnerable. Because in-house software is typically used in essential processes within companies, like industrial production lines, the impacts of exploitation can be massive. While it is most often only abused in highly targeted attacks when the attacker has already accessed the environment elsewhere, the damage can be profound when in-house software is exploited.

The Way Forward

The persistence of both threats and the patches that minimize them can overwhelm companies. Don't let perfection stall progress, however. Tenacity, best practice, and automation can meaningfully improve your security posture.

"60% of surveyed SysAdmins report their company either doesn't have a 3rd Party Patching software solution in place or they are unsure."*

Start Patching

The vital first step

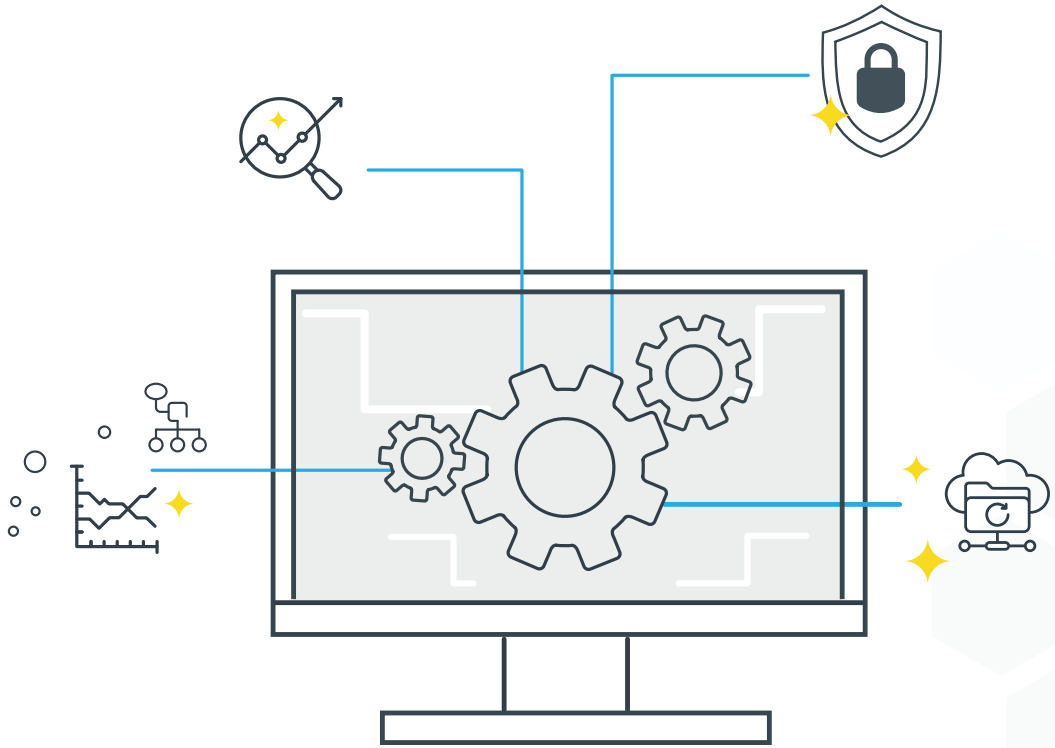
If you aren't patching third-party applications, it is important to get started now. Unless your company has a patch team on call 24/7, 365 days a year, best practice in 2023 requires the use of automated third-party patching software. The manual, in-house process of monitoring for updates across dozens of titles, deploying the package via a multistep process, and then pushing the final company-wide patch takes significant time and opens the door to delay and error. Downtime also isn't prudent.

* Data from The State of System Administration White Paper, which polled 500 SysAdmins globally. Access the white paper here.

Automate your Patching

Reduce human error

Third-party automation software provides constant, uninterrupted vigilance. After identifying the patches for you, the software enables automated packaging, testing, and system-wide update pushes whether it is mid-week, a weekend, or a holiday. Additionally, because 3rd-party patching solutions specialize in patching, the expertise provided by the professional patching solution greatly reduces human error within the packaging and deployment process.



“More business leaders are realizing that such repetitive tasks are better fulfilled by technology. Manufacturers realized this long ago when factories became automated, but enterprises have only recently started to implement software robots.”

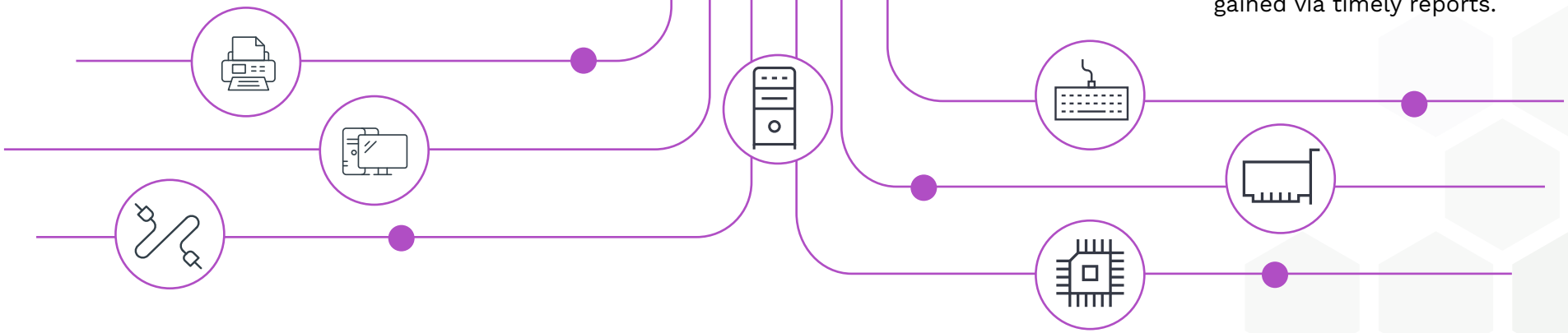
— Anthony Macciola, Forbes Technology Council, Forbes*

* Why You Should Consider the Cost of Human Error - Forbes

Shrink the Attack Surface

Security best practice requires timely 3rd party patching

Cybersecurity is improved greatly by timely, accurate 3rd party patching. This reduces the significant vulnerabilities that accompany exploited or expired versions.



Single Pane Patch Management and Reporting

A big win for both management and IT teams

With an automated patch management solution, you can see all the 3rd party patches in one place, keep track of patch installations and errors, and conveniently share patch data with management. IT Managers greatly value the visibility gained via timely reports.

Who We Are

We're obsessed with information technology and how to better manage it.

We are a dedicated group of Systems Administrators and tech-savvy product experts that love what we do and the IT community we do it with.

We empower organizations to better manage and support users and devices.

We are a rapidly growing software company with our solutions being used by thousands of enterprise organizations in more than 125 countries, impacting millions of devices and (more importantly) the people who use them. With our growing portfolio of tools, we empower IT departments at every single endpoint to do their best work.

Learn more about Recast Software here.
recastsoftware.com