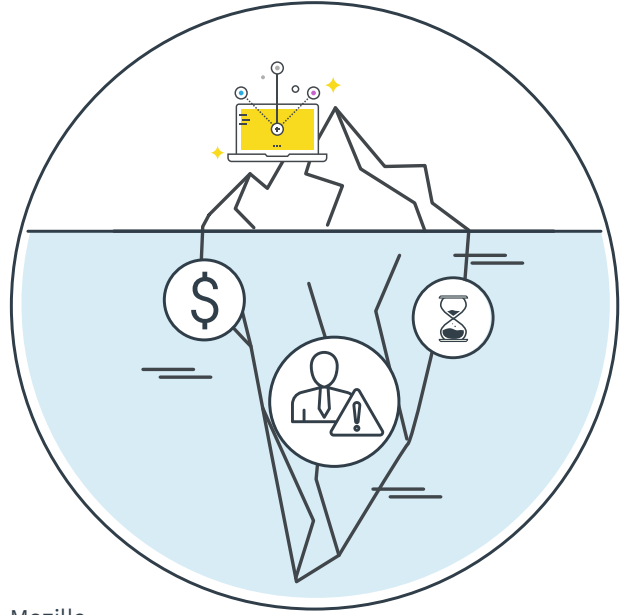
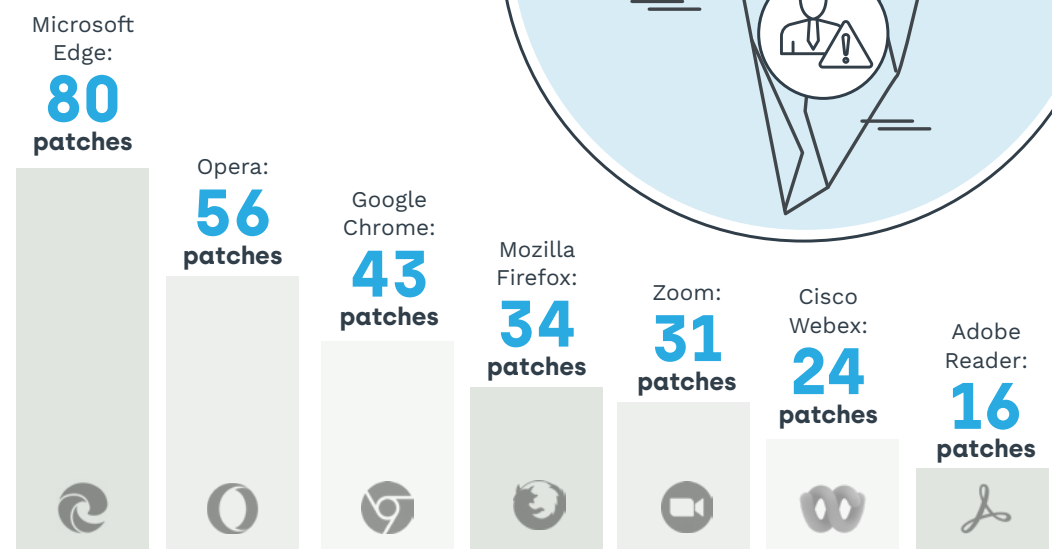


The Cost of Internally Patching

Explore the often-overlooked costs and risks associated with in-house patch management.



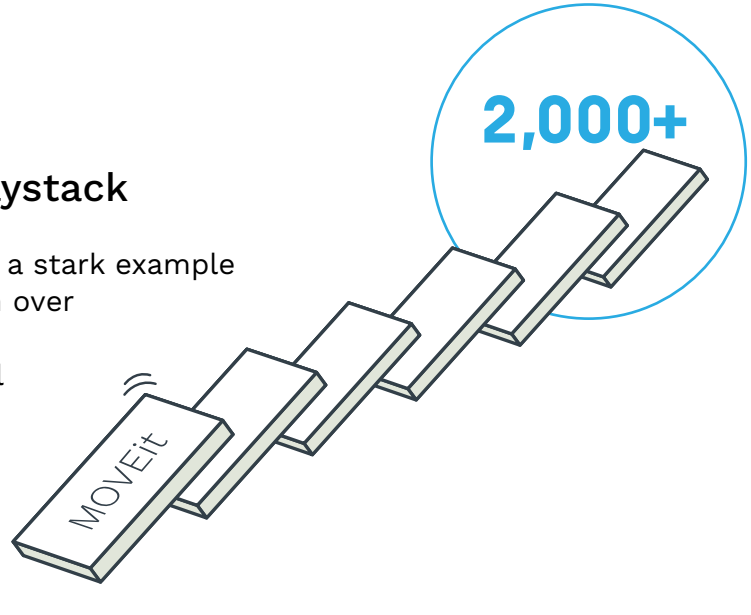
An Avalanche of Updates
2023 updates by software title



Patch Overwhelm

MOVEit as a Needle in the Update Haystack

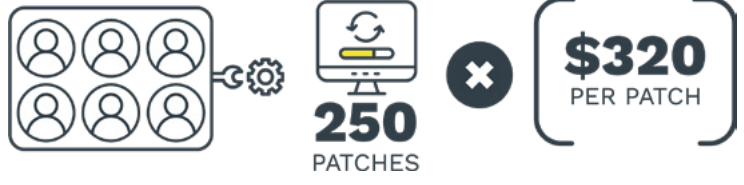
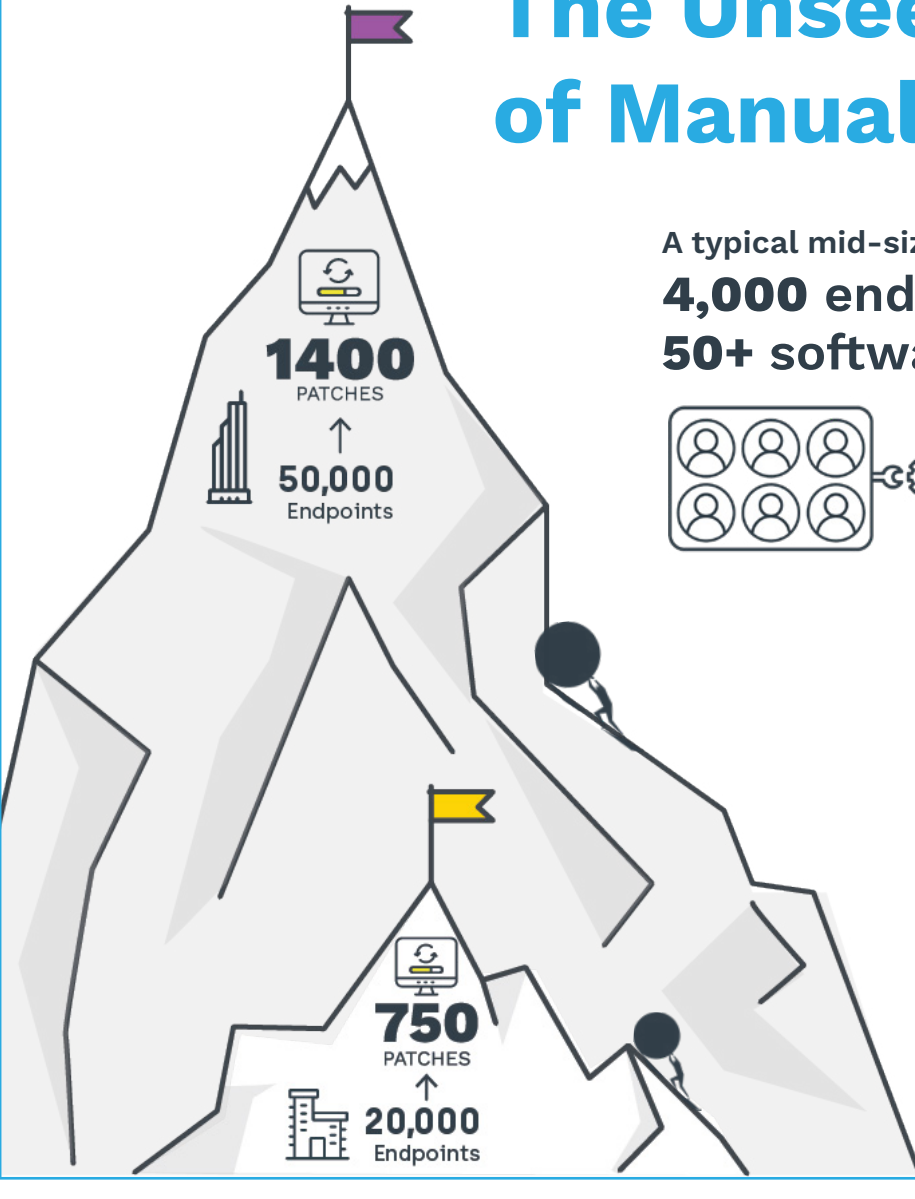
In 2023, the MOVEit system's vulnerability became a stark example of the cascading effects of security breaches. With over 2,000 organizations reporting attacks as a direct consequence, the incident underscores the critical need for rigorous and responsive patching protocols.*



* MOVEit, the biggest hack of the year, by the numbers - TechCrunch

The Unseen Costs of Manual Patching

A typical mid-sized organization manages **4,000 endpoints** and **50+ software applications**.



Larger organizations face greater complexity and costs.

Manual patching is costly, inefficient, and risky. Shift to automation for smarter patch management.

*These figures are conservative estimates based on customer feedback used to illustrate the scaling of resources and costs. Many teams require more resources and patch more applications at the endpoint counts listed.

A Never-Ending Patching Cycle

The in-house patching process is a relentless cycle of pilot testing, preproduction, and production patching—often disrupted by new patches before the previous ones are fully deployed. This ceaseless loop runs 24/7/365.

Holidays or weekends? Forget them—zero-day patches care not about time off, as underscored by urgent patch releases like the Google Chrome zero-day patch shared immediately after Thanksgiving in 2022.



Human Error in Patch Management

Human error remains an inescapable aspect of manual patch management. These errors can lead to dysfunctional applications, extended threat exposure, and increased security risks overall. 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)



Embracing Automation

The Smart Strategy to Mitigate Patching Pitfalls

Traditional patch management is inefficient and costly. Automation streamlines updates, reduces risks, and frees IT for strategic growth initiatives.



Learn more about RECAST SOFTWARE here.



About Recast Software

Recast Software is a crucial part of how teams create secure and compliant environments in an ever-changing IT landscape. Our software does this by seamlessly integrating with existing IT infrastructure to quickly remediate issues, ensure compliance, enhance security, and maintain clear visibility across all devices.