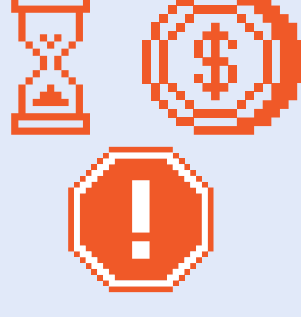


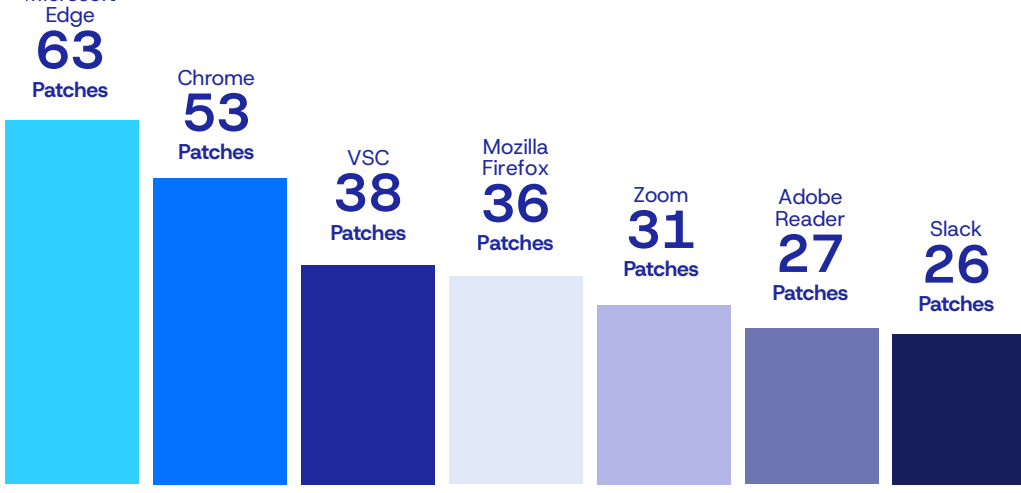
The Cost of Internally Patching

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



An Avalanche of Updates

2025 updates by software title

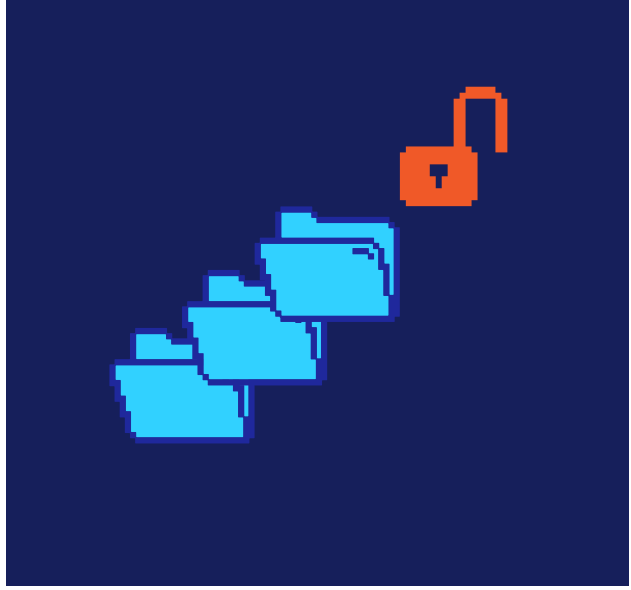


Patch Overwhelm

Cleo: A needle in the update haystack.

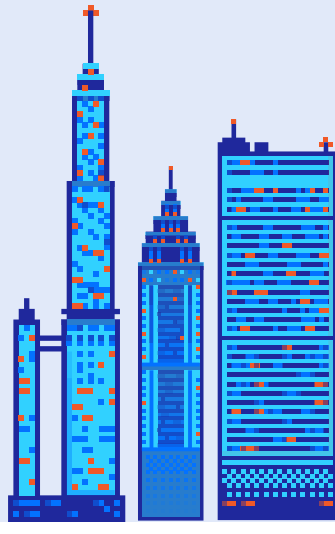
In December 2024, the Clop ransomware gang—the same group behind the MOVEit breaches—exploited a zero-day in Cleo’s managed file-transfer software (CVE-2024-50623). More than 200 organizations were posted to Clop’s leak site within a single month. Cleo’s first patch was incomplete and bypassed by attackers; an effective fix didn’t arrive until January 2025.

[BleepingComputer — “Clop ransomware claims responsibility for Cleo data theft attacks” \(Dec 2024\).](#)



The Unseen Costs of Manual Patching

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



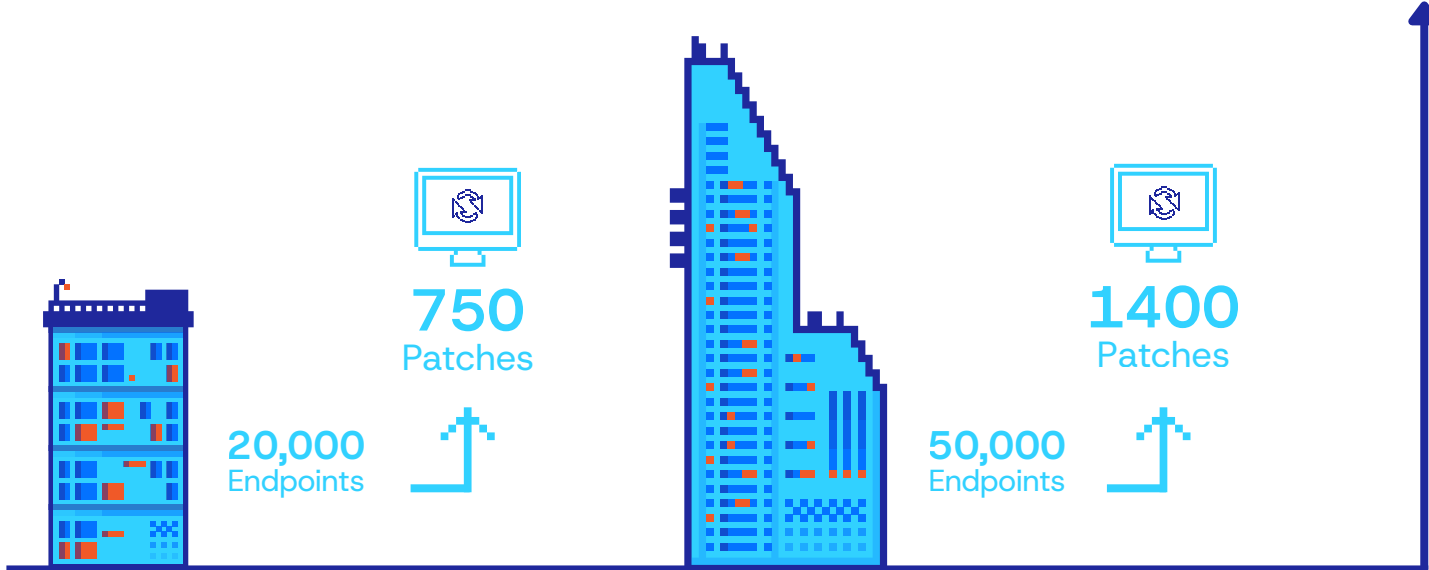
250 Patches



\$325
Per Patch

Larger organizations face greater complexity and costs.

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

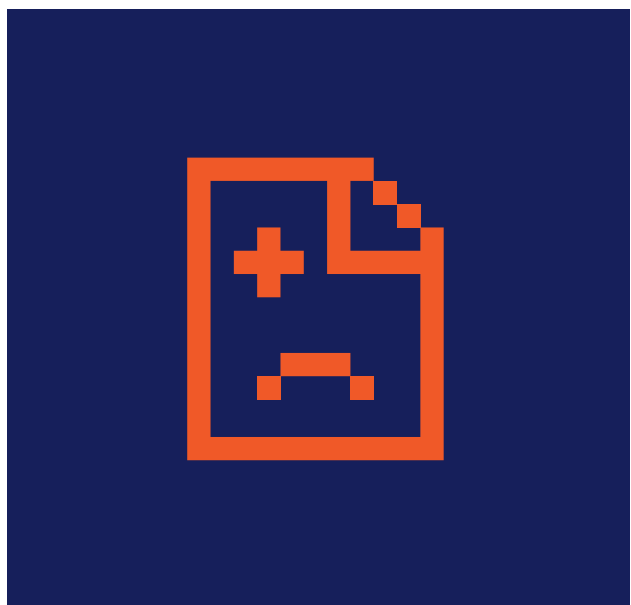


*These figures are conservative estimates based on customer feedback used to illustrate the scaling of resources and costs. Many teams require more resources and patch more applications at the endpoint counts listed.



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 don’t care about time off, as underscored by Chrome’s relentless stream of emergency fixes. By June 2026, Google had already shipped its fifth actively-exploited Chrome zero-day patch of the year (CVE-2026-11645).



Human Error in Patch Management

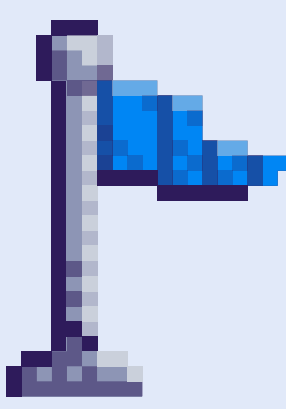
Verizon’s 2025 Data Breach Investigations Report found the human element involved in roughly 60% of breaches, while exploitation of vulnerabilities as an initial attack vector jumped 34% year-over-year. (Verizon 2025 DBIR)

[Verizon 2025 Data Breach Investigations Report.](#)

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.



6,500+

in the Recast third-party patching catalog—up from ~2,000 in early 2024.

World-class support

Endpoint and Application Management for the Modern Workplace