

Let's get a few facts straight.

To say that 2020 was a challenging year would be an understatement. As businesses scrambled to adjust to a new reality of remote work, another disaster loomed over their heads—cyberattacks!



242%
increase

in brute force attacks on remote desktop protocols (RDP), compared to 2019¹

1.7 million
unique malicious files

disguised as popular messenger and online conference applications that are used for work

11,121
aggregated vulnerabilities

disclosed in the first half of 2020²

\$3.86 million

was the global average for total cost of a data breach in 2020³

76%

of respondents believe the time taken to identify and contain a data breach will increase with remote working

So, businesses fought back.

They ramped up their network security, created more firewalls, arranged regular security trainings and did everything under the sun to boost their systems and networks' security.

But above all, they began **releasing patches and upgrades** faster than ever before.



Why?

Remember the bug fixes that you keep spotting on your application updates? They come from patches. They are a set of changes made to software or computer programs to update them, fix errors and to cut out security vulnerabilities.

In fact, Microsoft saw a 44% jump⁴ in the number of CVEs fixed just between January and April 2020, compared to the same period in 2019.

In short, releasing patches can



There's just one problem.

Completing a single patch cycle can take anywhere from a few weeks to months, especially when we look at the frequency of patch releases by product vendors, even with a dedicated workforce.

So, what do you do?

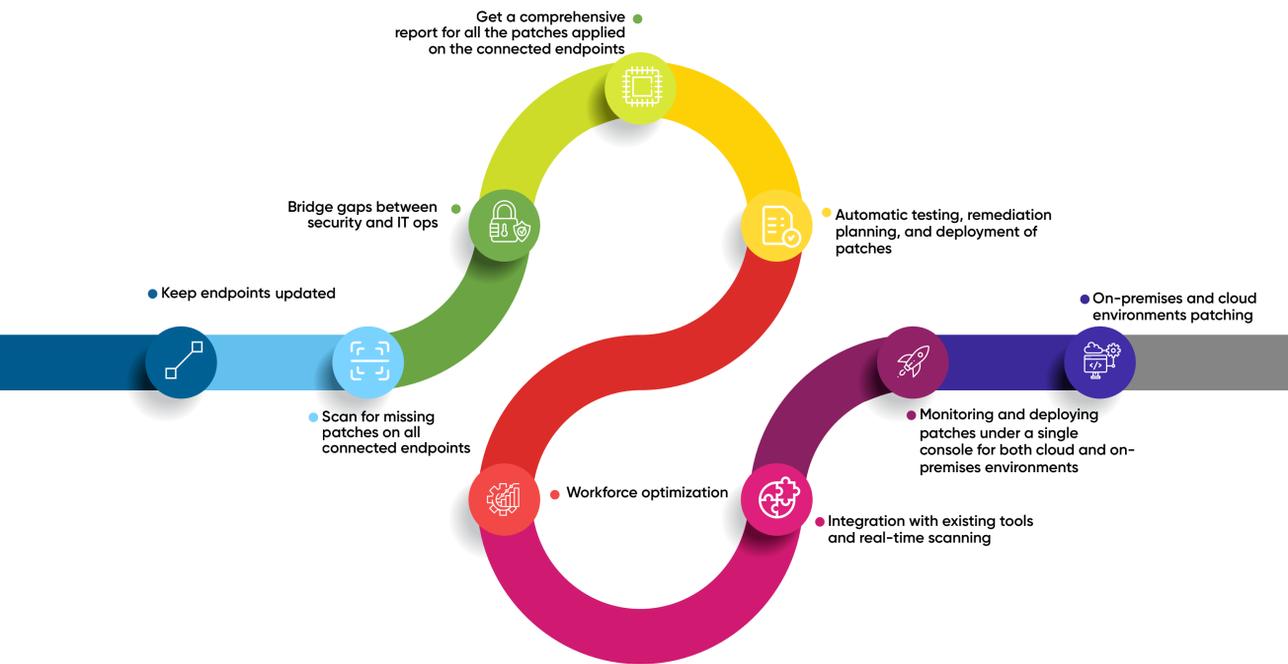


How do you ensure a consistent service and delivery within the prescribed SLA?

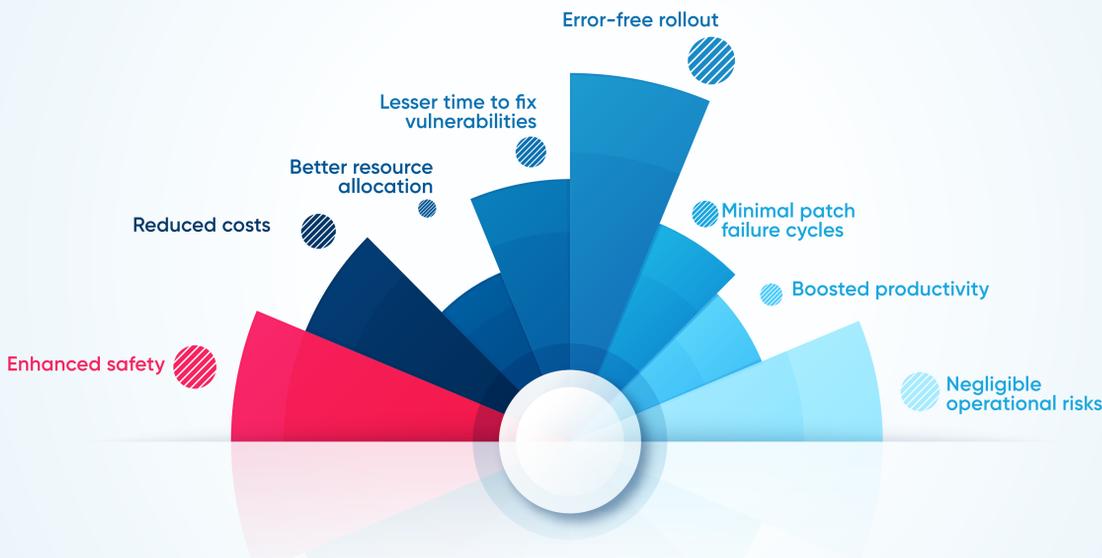


How do they keep your endpoints (servers/desktops, etc...) secure constantly?

Enter CT's Patch Management as-a-Service



For your business, it means



Wondering where to start? We've got you covered.

Long wait times are never fun, we know. Connect with us and let's kickstart your journey towards safer networks. What more? You get to try our solution for 30 days, absolutely free.

So what are you waiting for?

[Start Your 30-Day Free Trial Now](#)

[Learn more in our brochure](#)

Source

- <https://www.thehindubusinessline.com/news/world/wfh-opens-up-new-vulnerabilities-for-cybercriminals-report/article33381771.ece>
- <https://www.riskbasedsecurity.com/2020/08/27/new-research-2020-vulnerabilities-are-on-target-to-match-or-exceed-last-year/>
- <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf>
- <https://www.darkreading.com/application-security/microsoft-patches-113-bugs-3-under-active-attack/d/d-id/1337563>