

Patch Management as a Service



Keep your systems secure, compliant, and up to date with an effective patch management service based on a foundation of principles that forms a program, not a one-time event.

60% of breach victims said they were breached due to a known vulnerability where the patch was not applied.

Ponemon Institute Vulnerability Survey

Why is patch management important?

As an important part of a vulnerability management program, the purpose of a patch management program is to identify controls and processes that provide an environment that is secure against known vulnerabilities in operating systems and application software. Given proper attention, patch management provides:

Security. Often times, patches are released to fix vulnerabilities that have been found on hardware OS and applications, creating known vulnerabilities. By quickly implementing the patch for known vulnerabilities reduces the risk of cybercriminals finding the exploit.

Compliance. Regulatory bodies often require organizations to maintain a patch management program to maintain compliance standards based off industry standards.

Feature improvements. Patch updates often include feature updates that improve the function and user interface. This is why you pay a monthly fee for software maintenance.

System uptime. Ensure your OS and applications are kept up-to-date and running on the latest version to decrease risk of downtime.

Cybersecurity teams are not equipped enough to keep up, requiring the need to leverage the right tools to detect and patch in a timely manner.

Ponemon Institute Vulnerability Survey

Unfortunately there are many reasons companies don't keep up with patching. Including, but not limited to:

- Too many patches to keep up with.
- A manual and time-consuming process.
- Thinly-staffed organizations.
- Resistance of downtime.
- Risk of creating additional problems.

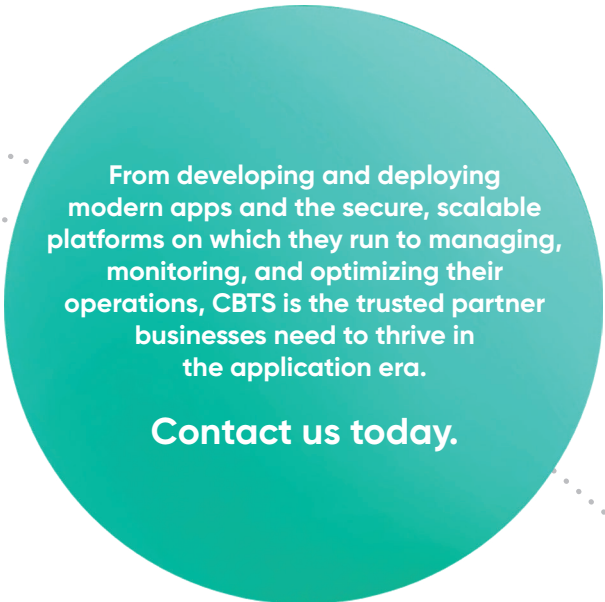
Patch smarter, not harder

Patch Management as a Service removes the chore and responsibility from your team and provides the value of time for them to focus on activities that result in business growth.

CBTS security experts will work your team to:

- Map current topology.
- Establish baseline of vulnerabilities.
- Apply all outstanding patches.
- Determine cadence of applying patches.
- Review ongoing critical patch escalation process.
- Provide an in-depth quarterly review.
- Maintain continuous ongoing assessment and monitoring.
- Provide audit and compliance analytics.

CBTS has some of the best and brightest professionals in the industry and is armed with industry-leading technology to help fill the security gaps specific to your organization. Contact a CBTS security expert today to learn how CBTS Patch Management as a Service can benefit your existing IT practice.



From developing and deploying modern apps and the secure, scalable platforms on which they run to managing, monitoring, and optimizing their operations, CBTS is the trusted partner businesses need to thrive in the application era.

Contact us today.



CBTS Patch Management as a Service
001230213 B