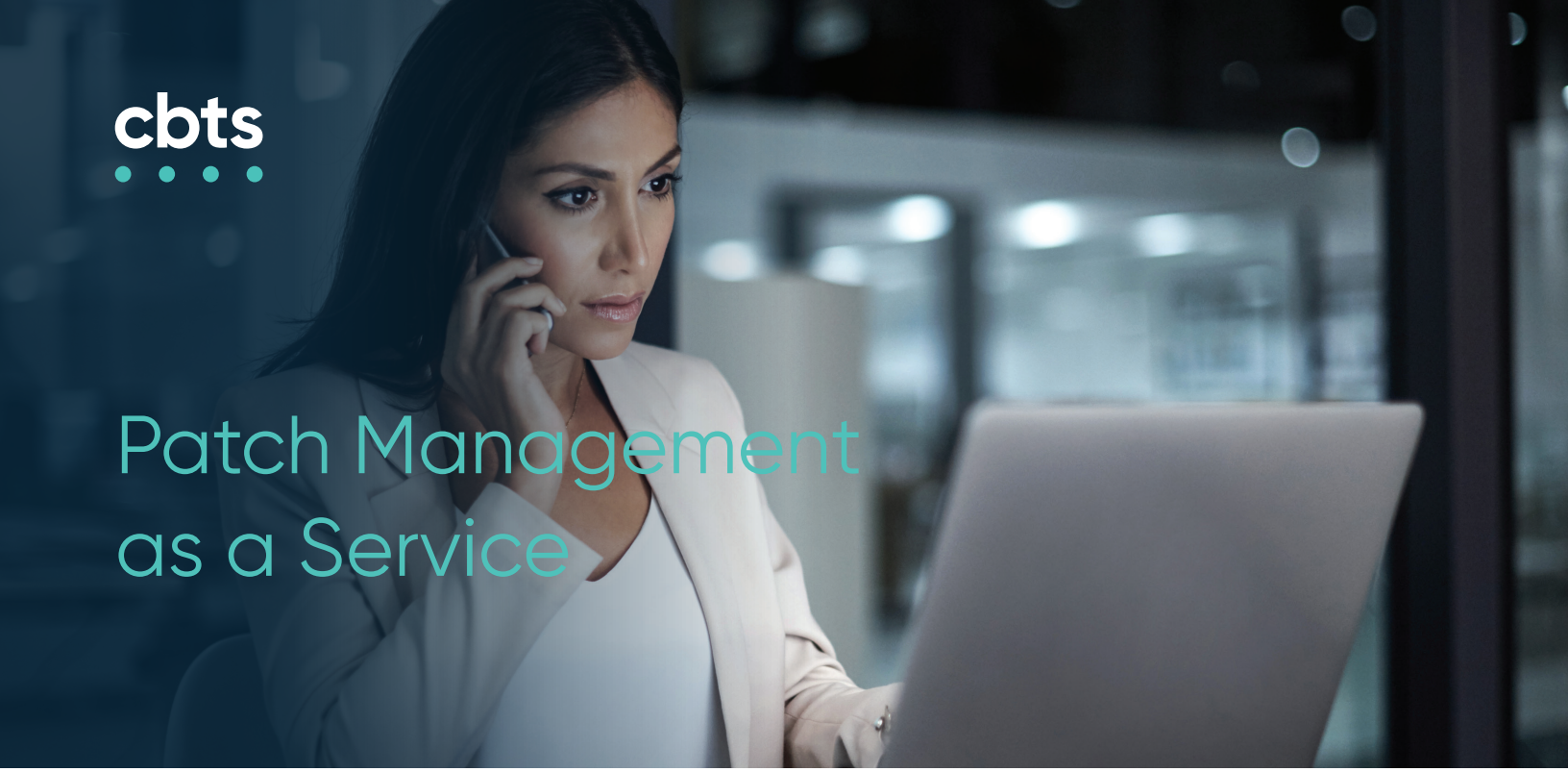

# Patch Management as a Service

Keep your systems secure, compliant, and up to date with an effective patch management service based on a foundation of principles that collectively form 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 in the OS or application layer. By quickly implementing the patch for known vulnerabilities you immediately reduce the risk of cybercriminals exploiting the vulnerability.

**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.

**Sustained Resilience:** A successful, secure foundation begins with a strong patching discipline. With digital footprints expanding, organizations can't afford to delay patching. A patch management program vastly improves resilience capabilities.

## Cybersecurity teams are not always equipped 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.
- The process is manual and time consuming.
- Organizations are staffed too thin.
- Resistance to 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 with 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, 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 productively augment your existing IT practice.

**Speak to a CBTS security expert today.**