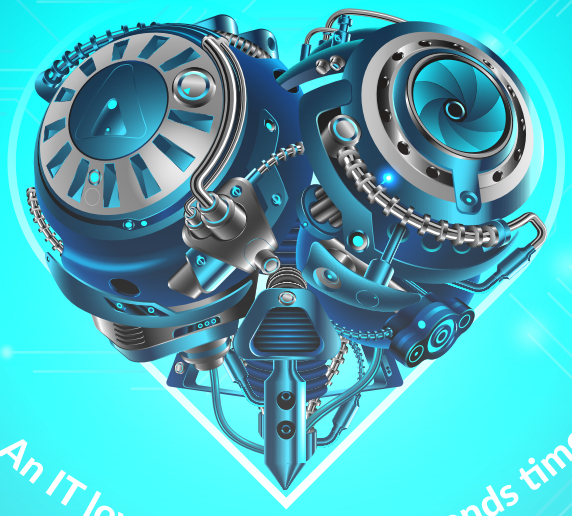
A Patch Made in Heaven



An IT love story that transcends time

"I LOVE PATCH MANAGEMENT," SAID NO ONE EVER.

While software patching is certainly a critical part of IT security, only about 45 percent of organizations have an automated patch management process. One of the main challenges is the sheer volume of software vulnerabilities and patches that need to be applied to fix them. If you're doing this manually, it's like experiencing Valentine's Day every day and having to constantly send out flowers and buy cards.

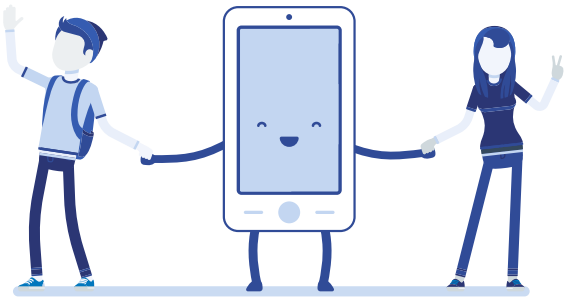
However, as breaches become more prevalent, IT professionals must find it in them to open their hearts and accept patch management for what it is — a way to create a robust security layer that involves the timely installation of patches. Time, of course, being the most critical element.

Of all the organizations that experienced a data breach in the last two years, 42 percent said that the incidents occurred because a patch wasn't applied for a known vulnerability.[1] Think of all the breaches that could have been avoided if only patching was embraced wholeheartedly.

Hackers love security flaws, or in other words, software vulnerabilities. A software vulnerability is a security hole or weakness found in a software application or operating system. Hackers exploit these weaknesses to deploy malware or to access the system and wreak havoc.

IT professionals need more than wine and roses to resolve and prevent this chaos from happening. True love and devotion means implementing an effective, automated patch management strategy to keep hackers out of their systems.

Showing love for patching can reduce the likelihood of a breach by **42%**



IT PATCH LOVE IS A BATTLEFIELD, BUT IT DOESN'T HAVE TO BE.

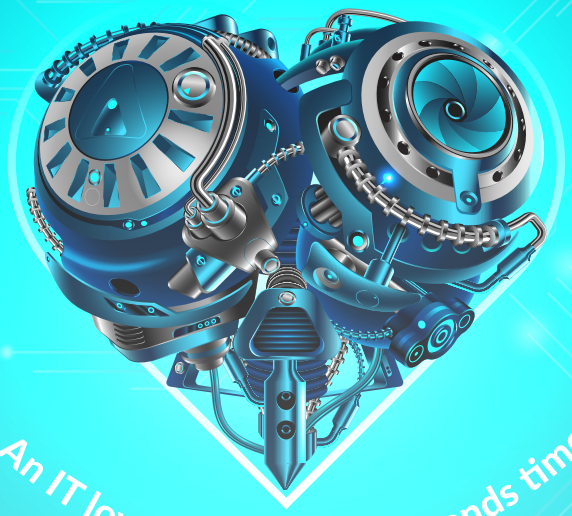
Any effective patch management strategy should have the following three critical components. Implement them and your systems and networks are sure to stay strong.

The first half of 2020 alone witnessed a 34 percent increase in new cyber vulnerability reports, rising to 9,799 from 7,318 in 2019.[2]

Kaseya®

TIP SHEET

A Patch Made in Heaven



1 MANAGE IT SECURITY FROM A SINGLE CONSOLE

Implement an "all-in-one" unified endpoint management solution that enables centralized management of the most common the security functions including patch management, antivirus/antimalware (AV/AM) deployment and management, and backup (BDR) management. Your patch management solution should allow you to keep every endpoint, both on- and off-network, up to date.

Large organizations usually deploy multiple tools for various operating systems, configurations and applications. However, they also often have a dedicated team to manage them. Midmarket enterprises lack these resources and must look for a unified solution that will save them time and eliminate the need for multiple tools. Labor savings can then be reallocated to other tasks that will benefit the business.

HOW KASEYA HELPS

Kaseya VSA is meant to be your main squeeze, providing unified management and comprehensive visibility along with scalable automation, so you can:

- Deploy, update and patch all of your Windows, Mac and third-party software from a single platform.
- Manage patching, AV/AM and BDR from a single platform.
- Leverage native Windows patching capabilities in VSA and, if desired, configure and enforce Windows update settings in VSA.

2 AUTOMATE PATCH MANAGEMENT

Tired of singing the same old love songs? Is the idea of putting so much effort into your relationship with patching exhausting? Four words: Set it and secure it. Leverage automation to implement proactive scans and schedule timely patches. This can certainly come in handy if you miss updates because of your tendency to daydream.

HOW KASEYA HELPS

Kaseya VSA enables scheduling of automated patches by:

- Time
- Computer
- Group or user-defined collections of computers

Then, Kaseya VSA

1. Scans networks for installed and missing security patches
2. Detects vulnerabilities
3. Maintains patch compliance

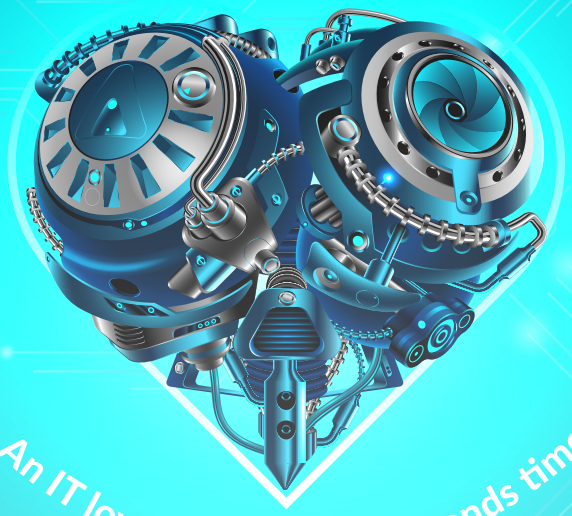
53% nerd love_

of the organizations said that their IT staff spends more time navigating manual processes than responding to vulnerabilities.[3]

Kaseya®

TIP SHEET

A Patch Made in Heaven



An IT love story that transcends time

3 BREAK DOWN SILOS

Did you know organizations lose approximately 12 days[4] when implementing a patch due to coordination issues between teams? Patch management love often lives in a vacuum and can be tedious and time-consuming when a company has organizational silos. Once an update is released, permissions are often required for installation, which might not be issued on time, creating a cycle of patch installation lags. That's when your love for patching starts to fade.

HOW KASEYA HELPS

VSA enables the creation of policy profiles for the automation of approval, review or rejection of patch updates. With VSA, you can simplify the patch update process by using standardized, scalable profiles to approve, deny or provide machine associations.

Fall in love with Patch Management and keep your systems and networks secure.

Request a Demo or Start a Free 14-Day Trial Today!

Sources

1 https://threatpost.com/large-orgs-plagued-bugs-patch-backlogs/158433/
2 https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox_Report_2020-VT_Trends.pdf
3 https://threatpost.com/large-orgs-plagued-bugs-patch-backlogs/158433/
4 https://public.dhe.ibm.com/common/ssi/ecm/55/en/55017055usen/2018-global-codb-report_06271811_55017055USEN.pdf