PARKER TECHNOLOGY SOLUTIONS

INSIGHTS · HOME & SMALL BUSINESS SECURITY

Why I Patch My Home Office with Action1 (and You Should Too)

Most computers get compromised through holes the vendor already fixed. A free tool closes that gap for homes and small businesses with up to 200 devices.

Written from 15 years as IT Director for the City of Lawrenceville and more than a year of running Action1 on my own machines. Not sponsored by Action1.

October 2026 parkertechsolutions.com
Kyle Parker, Parker Technology Solutions, Inc.

If you run a home office or a small business, the single most effective thing you can do for your security costs nothing: keep every computer patched. Action1 is the free tool I use to do exactly that, and it manages up to 200 devices at no cost.

Most successful attacks do not involve some brilliant new hacking technique. They take advantage of known holes in Windows, browsers, PDF readers and other everyday software that the vendor already fixed weeks or months earlier. The machine that gets compromised is usually the one nobody updated.

200

devices managed free, with no trial period or feature limits

$0

cost to patch a home office or small business under that limit

3

operating systems covered: Windows, macOS and Linux

5

desktops and laptops in my home it has patched for more than a year

Large organizations have layers of protection that most people never see. Beyond their own IT staff and enterprise tools, many rely on a Security Operations Center, or SOC. A SOC is a team of security analysts, either in-house or contracted, who monitor an organization's computers, servers and network around the clock. They watch for suspicious activity, investigate alerts, respond when something goes wrong, and track which systems are missing critical patches so they can be fixed quickly. The City of Lawrenceville had a SOC working alongside our IT team, and it was a significant part of how we stayed ahead of threats.

Home users and small businesses usually have none of that. There is no analyst watching at 2 a.m. and no one tracking which laptop missed last month's updates. That gap is why I want to tell you about Action1.

1. How I found it

I came across Action1 while I was IT Director for the City of Lawrenceville. I was researching cloud-based options at home in my spare time, looking for a way to fill a gap in our patching program.

At the time we were using an on-premises vulnerability management system. It was a capable product, but it was built around devices that sit on the internal network. A machine had to be connected to our network for the system to scan it and push updates to it.

That model did not fit a modern city. Remote users connect from home, from the field and from the road, and their laptops can go days without touching City headquarters. Those devices are the most exposed to risk, and at the time they were the hardest to keep current.

Action1 takes a different approach. Each device runs a small agent that reports to a cloud console over the internet, so it does not matter whether the laptop is in a home office, a coffee shop or a hotel room. If it has an internet connection, it can be scanned and patched.

Action1 looked like the right fit for the City. Then I noticed it is free for the first 200 devices, with no feature limits and no expiration, and realized I could use it at home too. I set it up on my home network. The City has well over 200 devices, so we purchased a license and deployed it there, and it closed the gap on our offsite devices.

Because it is free, I have kept it running at home ever since. It keeps all five of my desktops and laptops up to date, and I rarely have to think about it. I encourage you to do the same.

Keeping every machine patched helps protect your whole home network or small business, not just the one computer. It also matters when you bring a work laptop home to get something done. If the other computers on your home network are patched and up to date, that work laptop is far less likely to pick up an infection from one of them.

2. Vulnerability management in plain English

Vulnerability management is the habit of finding the weak spots in your software and fixing them before someone else finds them first.

Every program you run is made of millions of lines of code written by people, and people make mistakes. Some of those mistakes let an attacker do things they should not be able to do: run their own code on your machine, read your files, or install ransomware. When a security researcher or the vendor discovers one of these flaws, it is called a vulnerability.

Most serious vulnerabilities get a public ID number called a CVE (Common Vulnerabilities and Exposures), for example CVE-2026-12345. The CVE also gets a severity score from 0 to 10. A score of 9 or 10 usually means an attacker can take over a computer remotely with little or no help from the user.

The vendor then releases a fix, called a patch or update. Here is the catch: once a patch is public, attackers can study it to learn exactly what was broken. Within days, sometimes hours, automated tools start scanning the internet for machines that have not installed it yet.

> So the race is not between you and the hacker who found the flaw. It is between you and everyone who read about it after the patch came out.

A good vulnerability management routine looks like this:

1. **Inventory.** Know every device you own and what software is installed on it.
2. **Assess.** Compare that software against the list of known vulnerabilities to see what is missing.
3. **Prioritize.** Fix the most severe and most exposed issues first.
4. **Remediate.** Install the patches, or remove software you no longer need.
5. **Verify.** Confirm the update installed and the device restarted if required.
6. **Repeat.** New vulnerabilities are announced every week, so this never stops.

Windows Update covers part of this, but only for Microsoft products. The bigger blind spot is third-party software: Chrome, Firefox, Zoom, Adobe Reader, Java, 7-Zip, VLC and the dozens of other programs on a typical PC. Many of these update themselves only when you open them, and some never do. That is where most home and small business machines fall behind.

3. How Action1 works

Action1 automates every step of that routine from one web dashboard, for Windows, macOS and Linux machines.

- **A small agent on each device.** You install a lightweight program on each computer. It quietly reports what the machine has installed and what it is missing, and it carries out the updates you approve.
- **A cloud console.** You manage everything from a browser. There is no server to build and no VPN to configure, which is what solved the offsite problem at the City.
- **Inventory and vulnerability scanning.** The dashboard lists every device, its operating system, its installed applications and its last check-in time. Action1 matches that software against known CVEs and shows you which machines are exposed and how severe each issue is.
- **OS and third-party patching.** It installs Windows and macOS updates and also updates common third-party applications from its software repository, which is the part most free tools skip.
- **Automation policies.** You set rules once, such as "install critical updates every night" or "update third-party apps every Wednesday," and Action1 runs them on schedule. A device that was off or traveling picks up its updates the next time it gets online. Businesses can send updates to a small test group first so a bad patch does not hit every machine at once, and you decide whether machines restart automatically or prompt the user.

- **Reporting and remote tools.** You can see what was installed, what failed and what still needs a restart, which is useful evidence for insurers, auditors and clients. You can also connect to a machine to help a user, install or remove software, and run scripts across many devices at once.

In my house, the routine is simple. Each machine updates overnight on a schedule, and once a week I glance at the dashboard to confirm everything is green. If a patch fails, it shows up right there so I can deal with it.

4. Getting started

Setup takes well under an hour for a handful of machines, and most of that is walking from one computer to the next.

1. **Create a free account** at action1.com/free. Pick the data center region closest to you.
2. **Download the agent installer** from the console. It is tied to your account, so devices register to you automatically.
3. **Install the agent** on each computer. Within a few minutes each one appears in the dashboard with its software list and missing updates.
4. **Review the first scan.** Do not be surprised if the first report shows dozens of missing patches. That is normal, and it is the reason you are doing this.
5. **Create an automation.** Choose which updates to install (I start with all critical and security updates plus third-party apps), set a schedule outside working hours, and choose how reboots are handled.
6. **Check in weekly.** A quick look at the dashboard confirms updates are landing and flags any machine that has stopped checking in.

A few practical tips:

- Leave computers powered on, or asleep rather than shut down, during the update window so the schedule can run.
- Uninstall software you no longer use. Software you do not have cannot be exploited.
- Do not forget the family laptop or the old PC in the spare room. The forgotten machine is usually the weakest one on the network.

5. Why it matters even more now

Now that I have retired from the City and returned full-time to Parker Technology Solutions, keeping my own machines current is not optional. It is part of the job.

At the City, I had a team, a SOC monitoring our systems around the clock, layered security tools and a budget behind every endpoint. As a small business owner, I am the IT department. My laptops hold client documents, email, financial records and access to client systems. One unpatched machine could expose not only my business but the people who trust me with their information.

That is the same position most small businesses are in. Attackers know that small shops often have weaker defenses, and many of them go after the easy targets first. Cyber insurance carriers and larger clients are also asking more questions about how you protect your devices. Being able to show a patch report is a much better answer than "I think Windows Update is on."

The good news is that you do not need an enterprise budget to close this gap. If you have fewer than 200 computers, Action1 gives you the same patching tools larger organizations pay for, free, with no trial period and no feature limits. Set it up once, check it weekly, and you will have eliminated one of the most common ways computers get compromised.

Disclosure: I am not paid, sponsored or compensated by Action1 in any way. I use their free service at home, and the City of Lawrenceville became a paying customer while I was IT Director. This article reflects my own experience.

About the author

Kyle Parker is the founder and President of Parker Technology Solutions, Inc. (PTS), based in Gainesville, Georgia. He served 15 years as Information Technology Director for the City of Lawrenceville, retiring in 2026, and has worked with the City since 1989. Kyle holds the Certified Government Chief Information Officer (CGCIO) credential from UNC Chapel Hill and is a GMIS Emeritus member and NCLGISA member. Through PTS, he helps local governments and small businesses across Georgia and the Southeast put practical, affordable technology to work.

Sources

- Action1, free edition: action1.com/free
- Channel Insider, “Action1 Expanding Free Offering to Increase the Number of Endpoints,” February 2025
- Help Net Security, Action1 product showcase (Linux agent support), March 2026

Want help getting your machines patched?

I can help you set up Action1 for your home office or business, or take a second look at your overall security.

parkertechsolutions.com **kparker@parkertechsolutions.com** **404.310.5197**

© 2026 Parker Technology Solutions, Inc. · PO Box 1284, Gainesville, GA 30503 · Product details are accurate as of October 2026 and may change; check action1.com for current terms.