



An Extended Guide · No. 2084

Built-In Antivirus or Paid Protection? Securing Five PCs

When the free tools are enough,
and what paid protection adds

Tech Made Simple — Service Made Personal

BillsHomeTech.com · (330) 200-8042 · Atwater, Ohio

Free & printable — share it with someone who needs it



Book a visit —
billshometech.com/book

! Read this first — the two things that stop most attacks

Almost every small-business break-in starts in one of two ordinary ways: a password that got stolen or guessed, or a convincing email that talked someone into clicking or paying. You do not have to become a computer expert to stop most of it. Turn on two-step sign-in (also called multi-factor authentication, or MFA) everywhere you can, keep a backup you have actually tested, and give yourself permission to slow down before you click a link, open an attachment, or send a payment. That is the whole game, most days. That's worth remembering here, because no antivirus — free or paid — replaces two-step sign-in, a tested backup, and the habit of slowing down before you click.

Do you need to buy antivirus for five PCs?

It's one of the most common questions I get from small shops: we've got a handful of computers — do we need to pay for antivirus, or is the stuff that came with Windows and the Mac good enough? The honest answer is: for many small offices, the built-in protection is genuinely capable. For some, paid tools add things worth the money. This guide helps you tell which one you are.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. I've spent 30+ years helping folks and small businesses get comfortable with their technology, in plain language and at a kitchen-table pace. I don't sell software and I earn no commission, so this is just honest advice about where your dollars actually help.

Here's the idea to carry through: the free protection built into your computers has gotten genuinely good. Paid tools don't make a single PC magically safer so much as they help you **manage and watch** a bunch of PCs at once. Whether that's worth paying for depends on your size, your risk, and whether a rule or insurer is asking for it.

★ I'll tell you straight whether you need to pay

I have nothing to sell you, so I can look at your five (or two, or twenty) computers and tell you honestly whether the built-in protection covers you or whether a paid tool earns its keep. Call or text me at (330) 200-8042.

The whole guide, on one page

If you remember only these things, you'll make the right call for your shop.

- ❑ **Microsoft Defender Antivirus** (built into Windows) and the Mac's built-in protections are genuinely capable for a small office — when kept updated.
- ❑ **Keeping it updated** is the whole ballgame; an out-of-date tool, free or paid, protects nobody.
- ❑ **Paid tools** mainly add central management, reporting, faster response, and features an insurer or framework may want.
- ❑ If you have little IT help and low-risk data, built-in is often enough.
- ❑ If you handle sensitive customer data or have a compliance or insurance requirement, paid protection is often worth it.
- ❑ **No tool** replaces updates, two-step sign-in, tested backups, and not clicking the bad link.

! The dangerous myth: 'we have antivirus, so we're safe'

Antivirus — any antivirus — is one layer, and not even the most important one. Most break-ins start with a stolen password or a convincing email, not a virus. Buying a fancy tool and skipping two-step sign-in and backups is spending money on the wrong lock.

What you already have, for free

Before you shop, it helps to know how much protection came in the box — because it's more than most owners realize.

On Windows, **Microsoft Defender Antivirus** is built in and turned on by default. It scans files, watches for malicious behavior, and updates itself quietly in the background. Years ago free antivirus had a weak reputation; that's no longer a fair picture. For a small office that keeps it updated, Defender is a capable, real protector — not a placeholder.

On a Mac, protection is woven into the operating system itself. Features with names like **XProtect** and **Gatekeeper** check apps and files for known bad software and block untrusted programs from running. Apple updates these quietly too. Most small Mac offices don't need to add a separate antivirus to be reasonably protected.

✓ Make sure the built-in tool is actually on and current

On Windows, check Windows Security to confirm Defender is on and its definitions are up to date. On a Mac, keep the system updates flowing. Free protection only protects when it's switched on and current — which, happily, is usually the default.

What paid tools actually add

Paid protection isn't magic dust that makes one PC safer. It's mostly about managing and watching many PCs at once.

The paid category is often called **endpoint protection** or **EDR** (endpoint detection and response). On a single computer, a good paid tool and a well-maintained built-in tool catch much the same everyday threats. The difference shows up across a fleet of machines and over time.

- **Central management:** one dashboard to see and control every computer, instead of walking machine to machine.
- **Reporting:** records of what was blocked and when — useful proof for insurers, auditors, and your own peace of mind.
- **Faster response:** the ability to isolate or investigate a suspicious machine quickly, sometimes with experts watching.
- **Extra features:** things like detailed alerts and controls that frameworks or insurers increasingly ask about by name.

✓ The question isn't 'better,' it's 'do I need these parts?'

Ask yourself whether central management, reporting, and faster response actually solve a problem you have. On two or three computers you watch yourself, maybe not. On fifteen across three locations, they can be worth every penny.

Why this choice is worth getting right

Spend too little and you're exposed; spend on the wrong thing and you've wasted money that should have gone to a real gap.

The trap I see most isn't buying too little — it's buying antivirus and then feeling done. An owner pays for a well-known tool, checks the box in their mind, and never turns on two-step sign-in or tests a backup. Then a stolen password or a fake-invoice email gets them, and the antivirus was never going to stop either one.

So the real goal isn't to maximize what you spend on antivirus. It's to make sure protection is on and current on every machine, and then to put your attention and budget where the actual risk is: sign-in security, backups, updates, and training your people. Antivirus is one piece of that puzzle, free or paid.

! Put the free wins in place before you spend

Two-step sign-in, a tested backup, and current updates cost little or nothing and stop far more than any antivirus upgrade. Do those first. If budget remains and a paid tool fills a real need, then it's a smart next step, not a substitute.

Updated beats expensive, every time

If there's one thing that decides whether your antivirus works, it's whether it's current — not what it cost.

Antivirus recognizes threats partly from a constantly-updated list of what's bad. A tool that hasn't updated in weeks is blind to everything new. This is why an out-of-date paid product can protect you less than a well-maintained free one. Updates are the heartbeat; without them, the tool is just sitting there.

The good news is that both the built-in Windows and Mac tools update themselves automatically by default. Your job is mostly to not turn that off, and to make sure the computer itself gets its regular updates too — which our updates-and-end-of-support guide covers in detail. An unsupported, unpatched computer undercuts any antivirus running on it.

✓ Check that auto-updates are really on

Once in a while, open your security settings and confirm the protection is on and recently updated. It almost always is — but 'almost always' isn't 'definitely,' and a tool someone quietly disabled is a tool that isn't working.

When an insurer or a rule makes the choice for you

Sometimes the decision isn't really yours — a cyber-insurance application or a compliance rule asks for specific protection.

Cyber-insurance applications increasingly ask whether you have **endpoint protection** or **EDR** on your computers, and some security frameworks and industry rules expect it too. If a form asks specifically for EDR with central monitoring, a basic built-in antivirus may not be enough to answer 'yes' honestly — and as our cyber-insurance application guide stresses, an honest answer is the only safe answer.

If you're a tax preparer, take card payments, or fall under a rule like the FTC Safeguards Rule, there may be specific expectations about protecting and monitoring your systems. That's a legal and compliance question, not just a tech one — our guides on those rules explain what to ask, and you should confirm the current requirement with the right professional.

! A quick, important note

This guide explains the idea in plain English so you know what to ask about — it is general information, not legal or insurance advice, and it is not a substitute for reading the actual rule or policy. Laws and requirements change, and your situation may be different, so please confirm the current requirement with a lawyer, your insurance agent, or the agency itself before you rely on it.

Five quiet PCs, or sensitive data under a rule

The same five computers can point to very different answers, depending on what data they hold and what's asked of you.

If you're five PCs, no IT staff, low-risk data

A small shop with a few computers, nobody whose job is IT, and no especially sensitive customer records is often well served by the built-in protection — kept on, kept current, and backed by the free wins that matter more.

- Keep Microsoft Defender (Windows) or the Mac's built-in protection on and updating automatically.
- Put your energy and budget into two-step sign-in, tested backups, and current updates first.
- Glance at your security settings now and then to confirm protection is on and current.
- Revisit the question if you grow, start handling sensitive data, or an insurer begins asking for more.

If you handle sensitive data or face a requirement

If you hold a lot of customer, patient, or financial records, operate under a rule, or an insurer is asking for EDR with monitoring, paid endpoint protection often earns its place — the management, reporting, and faster response become real value, not just features.

- Look for central management so you can see every machine from one place, not walk desk to desk.
- Value the reporting — records of what was blocked are useful proof for insurers and auditors.
- Match the tool to the specific words on your insurance form or rule, so your 'yes' is honest.
- Remember it's still a layer — pair it with sign-in security, backups, and training, never instead of them.

★ Not sure which office you are?

Tell me how many computers you have, what kind of data they hold, and whether any form or insurer is asking for something specific — and I'll tell you honestly whether built-in covers you or a paid tool is worth it. Call (330) 200-8042.

Don't run two antivirus tools at once

More is not better here. Stacking antivirus products usually causes problems rather than solving them.

If you install a second antivirus alongside the built-in one, they can fight each other — flagging each other as suspicious, slowing the computer to a crawl, or leaving gaps while each assumes the other is handling things. The built-in tool is designed to step aside politely when a trusted paid product takes over, so you end up with one active protector, not two.

The practical rule: pick one real-time antivirus per computer. If you buy a paid endpoint tool, let it be the one in charge and don't bolt on extra 'free scanner' apps on top. More moving parts means more to go wrong and more that can quietly break without you noticing.

! Beware the 'free cleaner' and scareware trap

Pop-ups screaming that your PC is infected and pushing a 'free cleaner' are very often the actual threat. Real protection doesn't ambush you with alarms demanding a download or a payment. Stick to the built-in tool or one reputable paid product, and close those pop-ups without clicking.

The layer no antivirus can buy

The most effective protection on your five PCs isn't software at all — it's the people using them.

Most of what hurts small businesses walks right past antivirus: a staff member types their password into a convincing fake login page, or pays a fake invoice, or approves a two-step prompt they didn't request. No scanner catches a human being talked into opening the door. That's why a little training beats a lot of software.

Teach your people the few habits that matter: slow down before clicking a link or opening an attachment, verify any change to payment details by calling a known number, and never approve a sign-in prompt you didn't start. Our guides on fake invoices and on your one-page security plan turn those into simple house rules.

✓ Spend on people before you spend on software

A short, friendly conversation about spotting scam emails protects every computer you own and costs nothing. If you have a little budget and a little time, the training usually pays off faster than the upgrade.

If you decide to buy, choose well

I won't name brands — I don't take commissions and products change — but here's how to shop smart for a small office.

Decide first what you actually need: is it central management across several machines? Reporting for an insurer? A specific feature a firm names? Shop for the need, not the loudest marketing. A tool aimed at big enterprises can be overkill and a headache for a five-PC shop.

- **Fits your size:** built for small businesses, not just giant IT departments, so you can actually manage it.
- **Clear pricing per computer:** you know what five, or fifteen, machines will cost without surprises.
- **Readable reports:** you'll look at them, so they should make sense to a non-expert.
- **Real support:** someone to call when something looks wrong, especially if you have no IT staff.
- **Covers your mix:** Windows and Mac both, if your office runs both.

★ I can help you compare without the sales pressure

Since I don't sell any of it, I can sit with you, look at what each option actually does for a shop your size, and help you avoid paying for features you'll never use. Call (330) 200-8042.

Setting up protection so it actually works

Whether free or paid, protection only helps if it's set up and left running. A few checks keep it honest.

- ❑ Confirm protection is on and updating automatically on every computer — not just the one at the front desk.
- ❑ If you bought a paid tool, remove any leftover free scanners so two aren't fighting.
- ❑ Make sure alerts go somewhere a real person will see them — an inbox you check, not a dashboard nobody opens.
- ❑ Note which computers are protected, and with what, on your device list.
- ❑ Decide who responds if an alert fires — even if that's 'call Bill.'

The quiet failure is protection that's installed but ignored — an alert nobody reads, a machine that dropped off the dashboard months ago. A tool you watch, even loosely, is worth more than a pricier one you forget about.

✓ An unwatched alert is the same as no alert

Whatever you run, make sure its warnings reach a human. The best EDR in the world does nothing if the one email it sends lands in a mailbox nobody has opened since last spring.

What about servers, phones, and the rest?

Your five PCs aren't the whole picture. A quick word on the other things that run your office.

If you have an office **server** or shared storage, it deserves protection too — and it's often exactly where a paid tool's central view helps, because a problem there affects everyone. Phones and tablets are a different story: they're built to be locked-down by design, so the priority there is a screen lock, updates, and not installing sketchy apps, more than a traditional antivirus.

The through-line is the same for every device: keep it updated, keep sign-ins protected with two-step verification, and make sure anything holding your data can be recovered from backup. Antivirus is one layer on the computers; it isn't the thing that secures a phone or a server by itself.

✓ Count everything that touches your data

When you weigh built-in versus paid, count the whole set — PCs, Macs, a server, maybe a point-of-sale machine. A paid tool's value often depends on how many of these it can watch from one place.

The mistakes that waste money or leave gaps

Here are the slips I see owners make on both sides of this decision.

- **Buying antivirus and stopping there** — skipping the two-step sign-in and backups that matter more.
- **Assuming free means weak** — and spending on a fancy tool a small office won't use half of.
- **Turning off the built-in protection** and forgetting to put anything real in its place.
- **Running two antivirus products at once** and wondering why the PC crawls.
- **Letting a tool go out of date** — free or paid, stale protection protects nobody.
- **Nobody watching the alerts** — so a real warning sits unread for weeks.

! The costliest mistake is a false sense of safety

A business that believes it's protected lets its guard down — clicks faster, skips the backup test, ignores the odd sign-in prompt. The antivirus logo in the corner is not a force field. Keep your guard up no matter what you're running.

Making the call, simply

Boil it down to a few honest questions and the answer usually becomes obvious.

Ask yourself: How many computers am I really trying to watch? Do I hold sensitive customer, patient, or financial data? Is an insurer or a rule asking me for something specific by name? Do I have anyone whose job it is to keep an eye on this? Your answers point you to built-in or paid far more reliably than any product review.

For a few computers, low-risk data, and no special requirement, the built-in protection kept current is a defensible, honest answer — spend your effort on the free wins. The moment sensitive data, more machines, or a written requirement enters the picture, a paid tool's management and reporting start to pay for themselves.

✓ You can start simple and upgrade later

This isn't a forever decision. Many shops rightly start with built-in protection and the free wins, then add a paid tool when they grow or an insurer asks. Starting simple is not the same as starting unprotected.

Write down what protects what

A one-line record per machine makes insurance forms honest and troubleshooting quick.

For each computer, note what protection it runs, whether it's the built-in tool or a paid one, and that it's updating. Keep it with the same simple list where you track encryption and backups. When an application asks 'do you have endpoint protection on all computers?', you'll be answering from a record instead of a guess.

On your list	Why it helps
Which tool each PC runs	Answer forms honestly
Built-in or paid	Know what you're paying for
Updating? yes/no	Catch a stalled tool
Who sees the alerts	So warnings reach a person

✓ **Fold it into your one-page security plan**

If you keep the simple plan from our one-page security plan guide, add a protection column. One living page covering sign-ins, backups, encryption, and antivirus answers most of any insurance application by itself.

When 'antivirus' is the scam

Some of the nastiest traps wear an antivirus costume. Knowing them keeps you from inviting trouble in.

A browser pop-up warns that your computer is 'infected' and urges you to call a number or download a cleaner. A slick ad offers a free scan that finds dozens of scary problems. These are almost always fake — designed to frighten you into installing something harmful or handing over remote access or a payment. Your real protection never behaves this way.

The rule is simple: don't react to pop-ups that demand urgent action, don't call numbers they show you, and don't let anyone you didn't contact 'fix' your computer remotely. If a warning worries you, close the browser and check your actual built-in security settings, or call someone you already trust — like me.

! Real protection doesn't demand a phone call

No legitimate antivirus tells you to call a toll-free number right now or lose your files. That urgency is the tell. When in doubt, walk away from the screen and get a second opinion before you touch anything.

Where antivirus fits in the whole picture

Antivirus is one layer of several. It does its best work when the other layers are in place.

Picture the layers again: two-step sign-in keeps people out of your accounts; tested backups let you recover from nearly anything; updates close the holes attackers use; encryption protects lost laptops; and antivirus catches malicious software on the machines. Built-in or paid, antivirus is the layer for bad programs — important, but not a stand-in for the rest.

So don't let this decision loom larger than it should. Get protection on and current everywhere, decide honestly whether you need the management and reporting of a paid tool, and then spend the bulk of your attention on the sign-in, backup, and update habits that stop most trouble before antivirus ever has to.

✓ **Good-enough-and-maintained beats fancy-and-forgotten**

The best antivirus for your office is the one that's actually on, actually current, and actually watched. For many small shops that's the free one that came in the box — and there's no shame in that being the right answer.

A quick yearly review

Technology and your business both change. A short yearly look keeps your choice current.

- ❑ Confirm protection is on and updating on every computer and server.
- ❑ Reconsider the built-in-versus-paid question if you've grown or changed what data you handle.
- ❑ Re-read any insurance form or rule to see if the requirement has gotten tougher.
- ❑ Check that alerts still reach a person who'll act on them.
- ❑ Retire protection records for any computers you no longer use.

Tie this to your insurance renewal or tax time so it happens on a schedule. A business that outgrew its built-in protection two years ago, and never noticed, is exactly the kind of gap a yearly check catches early.

★ I'm glad to run the yearly review with you

If you'd rather not track this yourself, I can check every machine once a year, confirm the protection fits where your business is now, and give you an honest recommendation. Call (330) 200-8042.

Common Questions

The questions I hear most from owners weighing built-in against paid protection, answered plainly.

Q: Is the free antivirus in Windows really good enough?

For many small offices, yes — Microsoft Defender Antivirus is genuinely capable when it's on and kept current. It isn't a placeholder. Whether you need more comes down to how many machines you're watching, how sensitive your data is, and whether a rule or insurer asks for something specific.

Q: Do Macs even need antivirus?

Macs have strong built-in protections, so most small Mac offices don't need to add a separate antivirus for ordinary safety. The same rules apply, though: keep the system updated, use two-step sign-in, and keep tested backups. And a compliance or insurance requirement can still point you toward a managed tool.

Q: Will paid antivirus stop me from getting hacked?

Not by itself. Most break-ins come from stolen passwords and convincing emails that no antivirus catches. Paid tools help you manage and watch many machines, but they don't replace two-step sign-in, backups, updates, and careful people.

Q: Can I run a free tool and a paid tool together for extra safety?

No — running two real-time antivirus products at once causes conflicts and slowdowns. Pick one active protector per computer. If you buy a paid tool, let it take over and remove extra scanners.

★ Still not sure what your shop needs?

Give me a call and tell me about your setup — how many computers, what data they hold, what any form is asking. I'll give you a straight answer with nothing to sell. Call or text (330) 200-8042.

Your next step, today

You don't need to solve everything this week. One small action puts you ahead of most small shops.

Right now, on each computer, confirm the built-in protection is on and up to date — it probably is, and if so, that part is handled for free. Then look honestly at whether your two-step sign-in and backups are really in place, because those matter more than any antivirus choice. Only after those are solid is the paid-versus-free question worth agonizing over.

If your answers to the sizing questions lean toward a paid tool — more machines, sensitive data, an insurer asking — make that your project for the month, shopping for the need rather than the brand. Either way, write down what each machine runs so next year's decision starts from facts.

✓ One honest look beats a year of worry

Ten minutes confirming your protection is on and current, plus an honest glance at your sign-ins and backups, tells you more than any amount of shopping. Start there, and the rest gets simple.

You don't have to do this alone

You just have to remember that a friendly, patient person is one call away.

I hope this guide made protecting your office computers feel a little less daunting and a lot more doable. Keep it with your other business papers, come back to a page whenever you need it, and don't worry about memorizing anything.

When you'd rather have a hand, that's exactly what I do. I come to your business, work at your pace, and never make you feel rushed or silly for asking. A first visit is a flat \$99, and for the parts that don't need me on-site I can often help right on your screen for \$49. Every visit comes with a 30-day, come-back-free guarantee. I'm a tech helper, not a lawyer or your insurance agent — for the legal and insurance pieces I'll help you understand the questions and line up the right professional.

★ Bill's Home Tech — real help, close to home

Call or text me at (330) 200-8042, or visit BillsHomeTech.com. Serving Atwater and all of Portage County. 30+ years of patient, plain-English tech help — and if you're ever not 100% happy with a visit, I'll make it right or refund it. That's a promise. — Bill

Built-In vs Paid, at a Glance

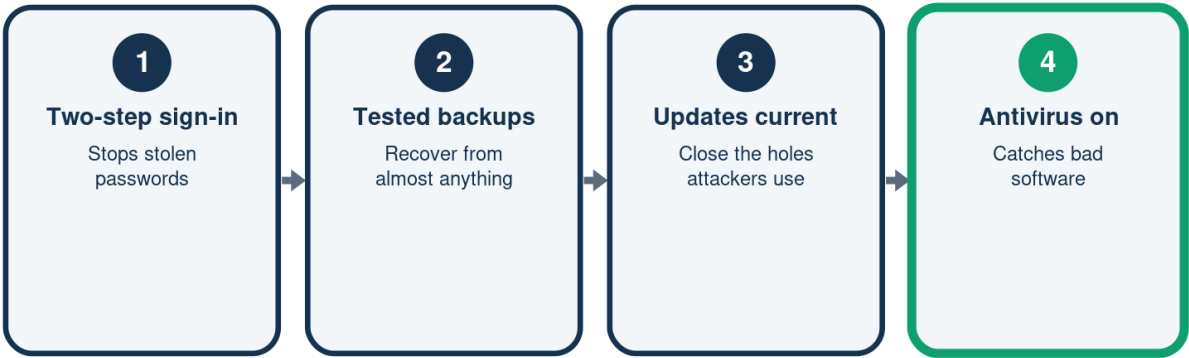
What each one really gives a small office

	Built-in (free)	Paid endpoint/EDR
Per-PC protection	Capable	Capable
Central dashboard	No	Yes
Reporting for forms	Limited	Yes
Faster response	On your own	Tools/experts
Cost	Free	Per computer

On one PC they're close; paid value is in managing many at once.

Antivirus Is One Layer

Put the free wins first



No antivirus replaces sign-in security, backups, and updates.

What Paid Protection Adds

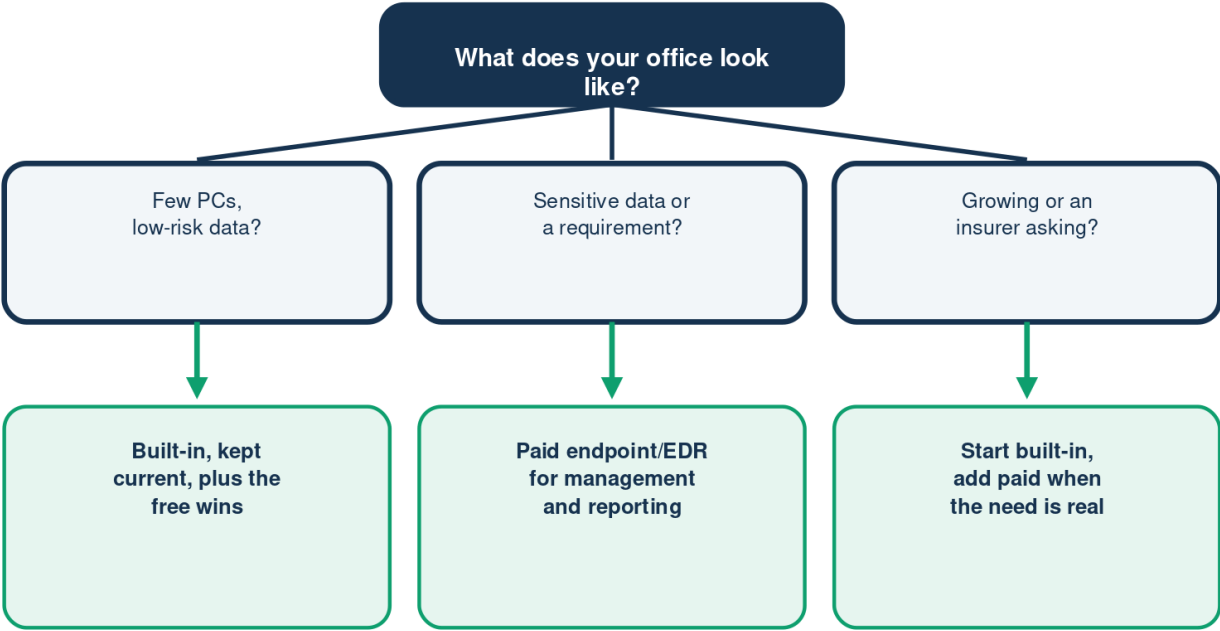
Ask if you actually need these

	What it adds	Worth it when
Central mgmt	One dashboard	Several machines
Reporting	Proof of blocks	Insurer or audit
Faster response	Isolate fast	Sensitive data
Named features	Checklist items	A form asks

Shop for the need, not the loudest marketing.

Built-In or Paid for Your Shop?

A few honest questions decide it



Whatever you pick, no antivirus replaces MFA, backups, and updates.

Illustration - a schematic, not to scale. Your setup may differ.



Need a Real Person?

You do not have to remember all of it.
You just have to remember you can call.
Friendly, in-person tech help -- I come to you.

BILL'S PROMISE

If you are not 100% happy with a visit, I will
make it right -- or refund it. No awkwardness,
no fine print. That is how I would want to be treated.

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

— Bill

Prefer help without a visit?

Bill can screen-share and fix many things remotely — a flat \$49, free for Support Plan members.



A Note From Bill

A quick note from Bill.

I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that comes from using these guides. Thanks for reading, and stay safe out there.

— *Bill*



Book a visit —
billshometech.com/book

Use of these guides is subject to our Terms of Use (billshometech.com/terms-of-use).

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

For general information only — not professional advice. Use at your own risk. For electrical, gas, water, or ladder work, please call a licensed professional. — Bill's Home Tech