ONBOARDING · STEP 2 DELIVERABLE

Environment Baseline & 90-Day Plan

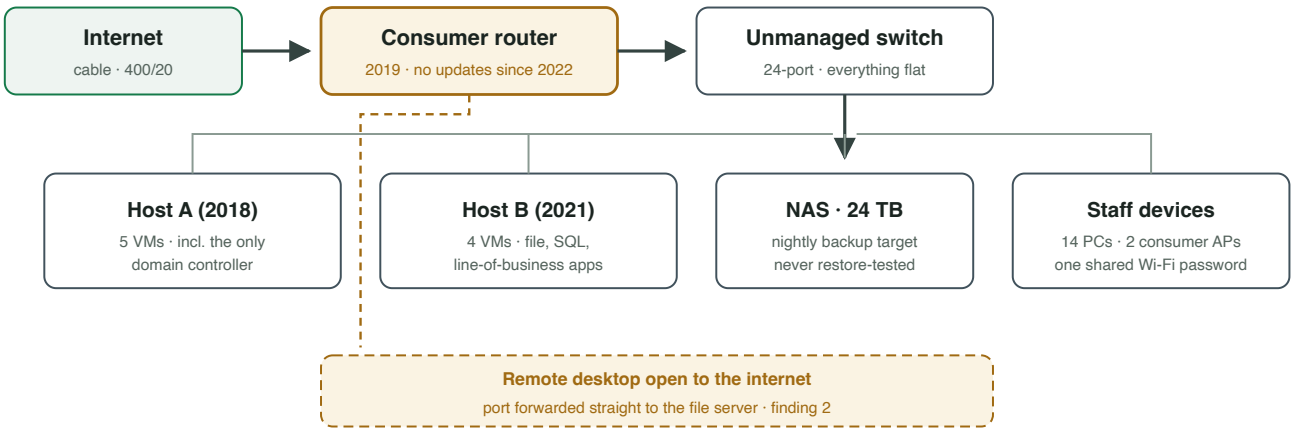
Prepared October 6, 2025, before any change was made

> **This is a sample.** Same fictional company as the sample monthly report, seen here at onboarding, before anything was fixed. Together the two documents show the before and the after. A real baseline is produced from one afternoon of guided, read-only discovery. Nothing is changed while it's written.

CLIENT	STAFF	FOUND	OVERALL
Sample Client, LLC	17 people, one office	2 hosts · 9 VMs · 1 NAS · 14 PCs	Typical, fixable

The quick map

WHAT'S ACTUALLY ON THE NETWORK



This first map is deliberately rough. The full diagram, with addressing and per-system detail, gets built during month one and maintained from then on.

What the first pass found

QUICK PASS · DETAIL COMES WITH THE WORK

None of this is unusual. This is what most small business networks look like, and all of it is fixable on a schedule, without drama. Each item below becomes a line in the plan on page 3.

1 · PERIMETER **The firewall is a consumer router that stopped receiving security updates in 2022.** It has no intrusion prevention and no DNS filtering. The replacement is a business-grade pfSense firewall. I spec the exact unit, you order it at cost, and anyone on site plugs it into power and internet and enables remote access. From there I configure and cut over remotely; both protections are live the same evening.

2 · PERIMETER **Remote desktop to the file server is reachable directly from the internet.** A port forward, probably from an old vendor visit. This is the single most common entry point in small-business ransomware cases. It moves behind a VPN in week one.

3 · PATCHING **No patch schedule exists.** The hypervisors are on a 2023 release and the Windows servers average fourteen months behind. Two catch-up windows bring everything current; a monthly cadence keeps it there.

4 · BACKUPS **The nightly backup reports success and has never once been restored.**

5 · ACCESS **One shared admin password, used everywhere, known to at least one outside vendor.** Two accounts believed belonging to former employees (not logged into for 8 months) are still active. Individual admin accounts and a cleanup close this out.

6 · RESILIENCE **There is exactly one domain controller, and no monitoring anywhere.** If a disk dies or the backup silently stops, the first alert is a user who can't work. A second domain controller and monitoring fix both.

> **Why the firewall matters more than it looks:** most ransomware arrives as one ordinary click on a convincing email, and the malware's first move is to quietly call its operator's server for instructions and encryption keys. That call home is a genuine chance to stop the whole thing, because a firewall that filters known-bad destinations and inspects traffic can cut it off even after the click. Today, nothing on this network would notice that call, let alone block it. Closing that gap is the first job on this plan.

What's already in good shape

WORTH SAYING OUT LOUD

HARDWARE Both server hosts are healthy and mid-lifecycle. No hardware purchases are needed this year, and probably not next year either.

STORAGE The NAS is well sized and its disks test clean. At the current growth rate the space lasts for years.

DOMAIN SERVICES Domain services tested healthy (note no current replication).

INTERNET Bandwidth is comfortably adequate for the business, with room to grow. Keep the plan you have.

The first 90 days

EVERY CHANGE IN A WINDOW · ROLLBACK STAGED FIRST

WHEN	WHAT HAPPENS	YOU'LL NOTICE	YOUR COST
Weeks 1 and 2	You order hardware I designate for you, then your on-site contact plugs it in and sets up access; I configure and set up the pfSense firewall remotely, intrusion prevention and DNS filtering live from night one. The open remote desktop closes; remote staff get proper VPN profiles. Old router stays on a shelf as the rollback.	One evening cutover, ~20 min of internet downtime	Firewall hardware, ~$500 at cost; labor in the flat onboarding quote
Weeks 3 and 4	Patch catch-up in two scheduled windows: hosts first, then the VMs. Snapshots staged before each window.	Nothing, both windows run overnight	In the onboarding quote
Month 2	Backup overhaul: verification, the first real restore test, and a weekly offsite copy. A second domain controller comes up on Host B.	Nothing	In the onboarding quote; offsite storage billed by the vendor, in your name
Month 3	Access cleanup: individual admin accounts, stale accounts disabled. You receive the full environment map and runbook.	Your first monthly health report	In the onboarding quote

After that, steady state: with eleven VMs once the second domain controller and monitoring come up, this environment fits the **Complete tier ($1,000/month)**. Maintenance would run as agreed on the second Wednesday of each month at 10:00 PM. The one-time project work above is quoted flat, in writing, before anything starts.

The kickoff call

ONE MEETING, ON PURPOSE

Once you approve the plan, onboarding starts with a video call. You meet me, the engineer who will hold your keys. We walk this document together, and name your on-site contact: whoever will plug in hardware on the rare day something physical needs doing. It might be good to consider that person for the call as well. That is the only part of the service that needs local hands. Ask anything you like while we're at it, technical or not.

It's also usually the end of the stressful IT meetings or cost concerns about infrastructure. The service is built to be quiet: the monthly report does the talking, questions get answered in writing, and once a year I'll offer a short strategic review call to look ahead at budget, growth, and hardware lifecycles. What you keep is the peace of mind of knowing the backups ran, the patches landed, and an experienced engineer checked it all, every month.

Dave Walter
Walter Infrastructure · Principal Engineer