dental IT

AN ANALYSIS OF 192 ON-SITE IT AUDITS · 184 PRACTICES

The hidden state of dental-practice IT

What 184 dental and orthodontic practices actually look like behind the reception desk: the software, the servers, the ageing PCs, the open back doors and the quietly failing backups, all drawn from years of Dental IT's on-site infrastructure audits.

184 PRACTICES · 192 DOCUMENTS GATHERED OVER ~5–7 YEARS

TEXT-MINED & HAND-CHECKED ALL SITES ANONYMISED

Dental practices are small businesses carrying hospital-grade obligations: patient records, clinical imaging, card payments, and a regulator that expects all of it to be secure and available. This piece looks under the bonnet of 184 of them. The audits were never meant to be a tidy dataset; they were working documents written in different styles, in a programme that ran over **at least five to seven years** (roughly 2016–2025), some a dozen pages long, some a few scribbled lines. Every figure here is therefore a **broad-brush estimate, not a precise census**. And because the work spans so many years, anything time-sensitive (broadband speeds, which Windows version still counts as "current") is best read against the date of each visit (see *How to read this*, below). Names, addresses and domains have been stripped; nothing below identifies a real practice.

184
dental & orthodontic practices reviewed

45%
flagged slow or unreliable internet, the most common complaint

48%
ran Windows or server software their auditor flagged out of date at the time

~1 in 4
used generic shared logins or weak passwords

How to read this. Each record is an on-site review of one practice's IT: cabling, network, PCs, server, backups, phones, practice-management software and more. They arrived in three depths: long narrative reports, mid-length checklists, and short site notes. The headline *count* of 184 practices uses everything; the *problem rates* below are calculated over the 137 audits with enough written detail to judge, and infrastructure splits (software, broadband, phones) use only practices where that detail was recorded. Because fields were often left blank, **absence in the notes doesn't prove absence on site**, so these numbers tend to *under*-count problems, not over-count them.

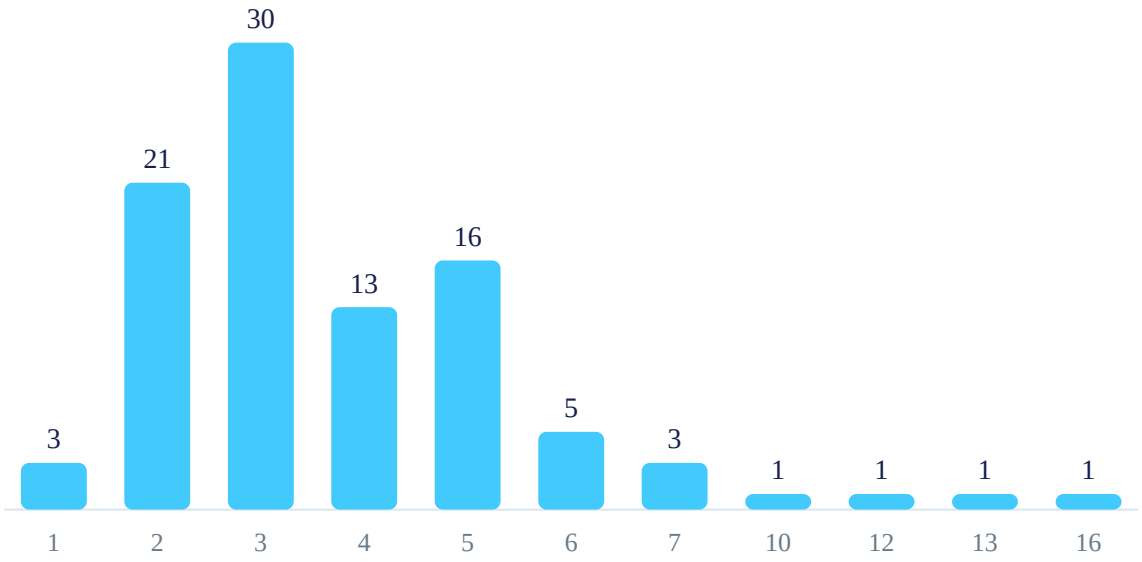
Mind the span. These visits took place over at least five to seven years, so time-sensitive findings (broadband speeds, which operating systems count as "current") should be read against *when* each audit happened: a 15 Mbps line or a Windows 7 PC meant something milder in 2017 than in 2024. Crucially, the auditors recorded at the time whether kit was out of date or underpowered, so the "out of date" and "too slow" calls here are **contemporaneous professional judgments, not hindsight**.

01 Who these practices are

These are overwhelmingly small, owner-run clinics rather than corporates. Where size was recorded, the typical site had **3–4 surgeries** (median 3, mean 3.9), with a long tail up to 16 for the larger group and specialist sites.

PRACTICE SIZE: NUMBER OF SURGERIES

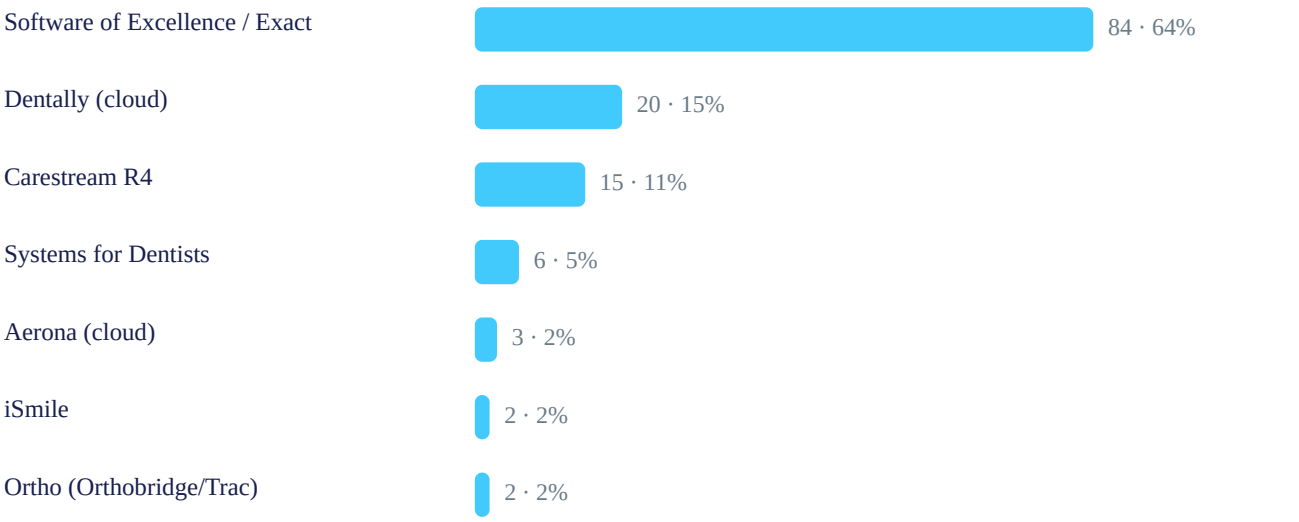
N = 95 · MEDIAN 3



The software running the front desk tells a clear story of dominance. **Software of Excellence's "Exact"** appears in about 64% of practices where the system was named, the long-standing incumbent by a distance. Cloud-native systems like **Dentally** and **Aerona** cluster in the newer audits, a quiet signal of where the market is drifting.

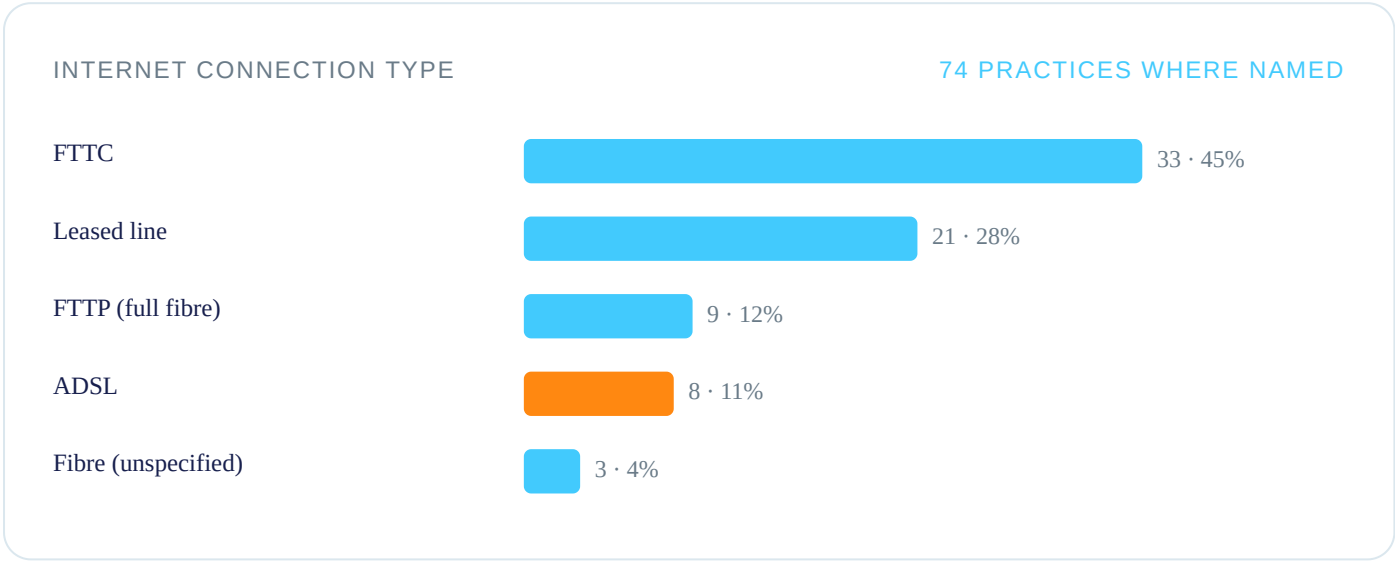
PRACTICE-MANAGEMENT SOFTWARE

132 PRACTICES WHERE NAMED



02 The connection problem

More than anything else, these audits were triggered by things being **slow**. Slow or unreliable connectivity was the single most common complaint, flagged in **45%** of detailed audits, and the data shows why.

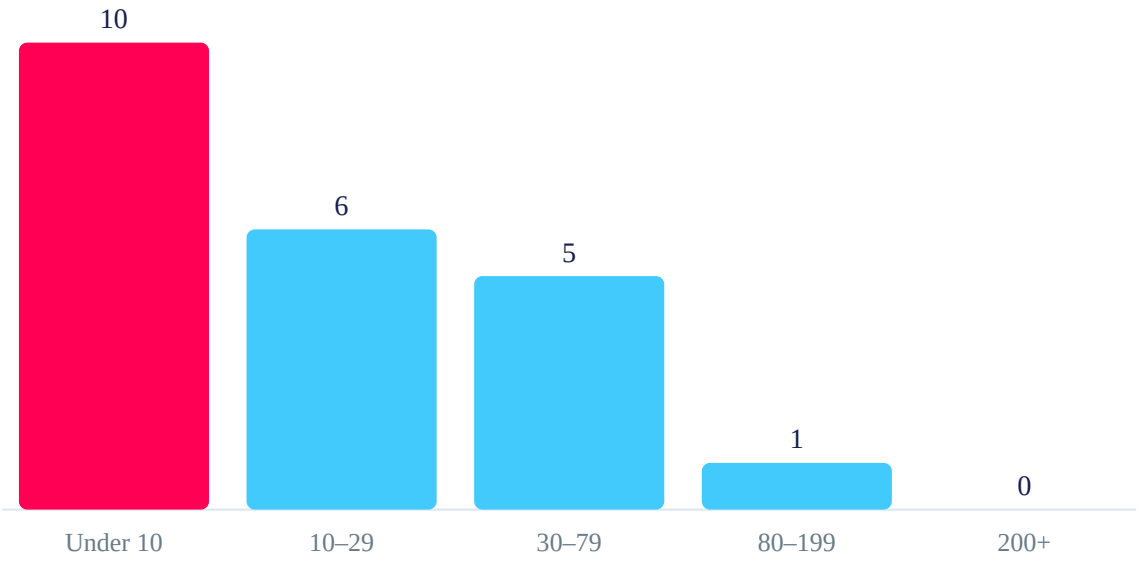


Where a connection was named, fibre-to-the-cabinet (FTTC) is the workhorse, with a healthy minority on proper leased lines, but ageing copper **ADSL** still turned up in practices running cloud software, card machines and digital X-rays over it.

When a speed was actually measured, the numbers were sobering. Among the 22 practices with a recorded figure, the **median download was just 14 Mbps**, and **10 of 22** were limping along below 10 Mbps, for an entire clinic. Some of these readings come from earlier in the period, when expectations were lower; even so, a whole clinic sharing under 10 Mbps was firmly inadequate in any of these years, and the auditor said so on the day.

MEASURED DOWNLOAD SPEED (MBPS)

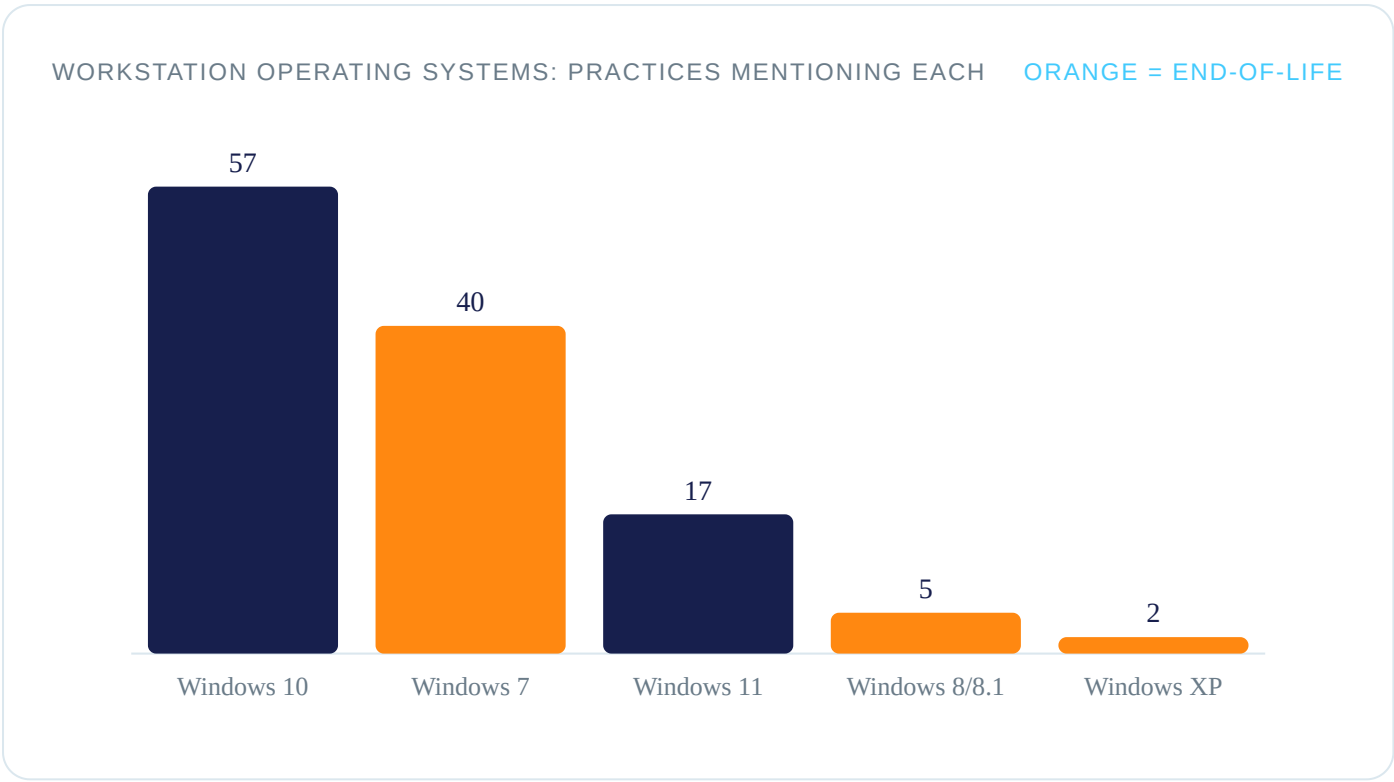
N = 22 · MEDIAN 14



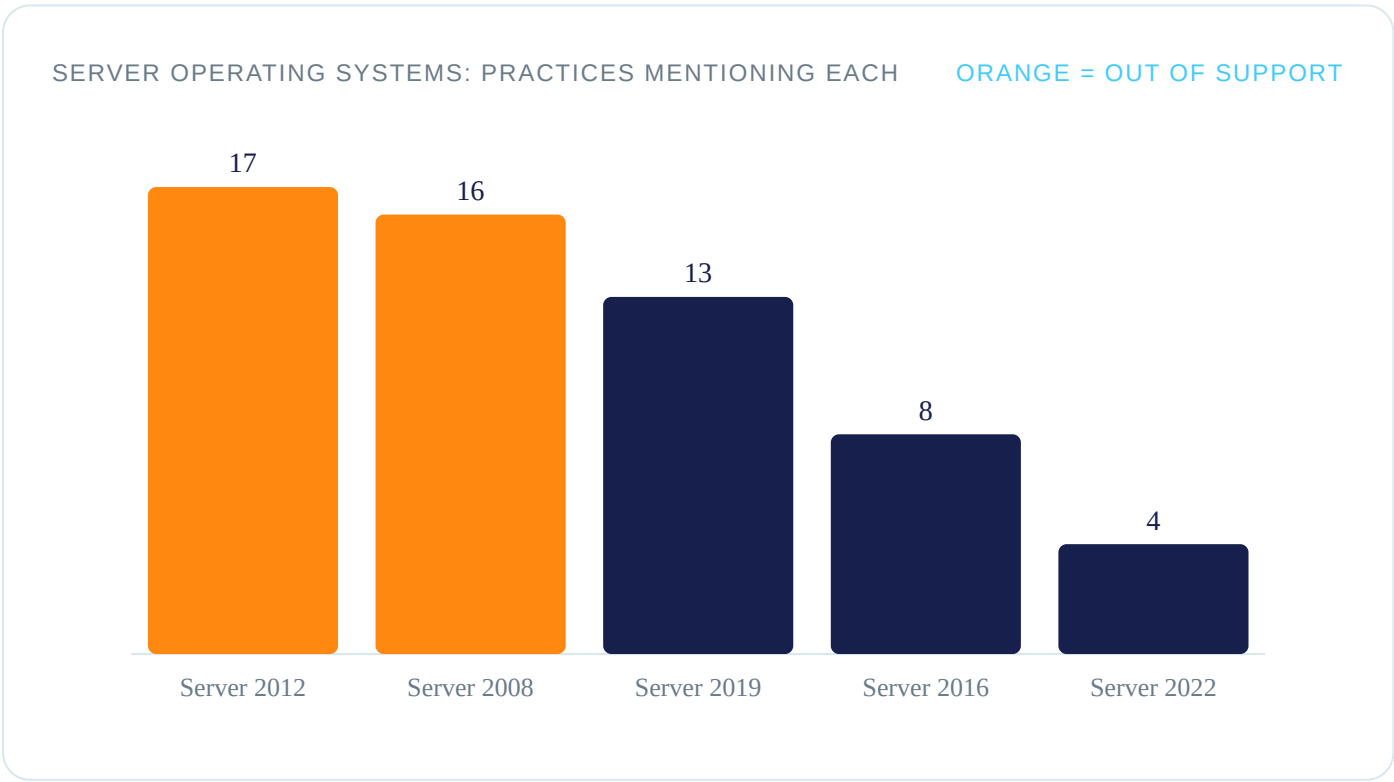
> **Across these years, a striking number of practices were running modern, data-hungry clinical software over a broadband line you'd be unhappy with at home.**

03 An ageing estate

The hardware tells the same story as the broadband. Windows 10 is the most common desktop, but **out-of-date operating systems are everywhere**: Windows 7 (retired by Microsoft in January 2020) still turned up in 40 practices, and a couple were still running Windows XP. Because the audits straddle that 2020 retirement, some of those Windows 7 sightings were of a still-supported-but-ageing system and some of a genuinely expired one. In each case, though, the auditor recorded where it sat on that curve.



Servers are worse, because they're harder to replace. Out-of-support Server 2008 and 2012 between them still appear across a swathe of sites: practices holding live patient data on an operating system that no longer receives security patches. The calendar matters here too: Server 2008 left support in 2020 and 2012 in 2023, so the same finding bites harder the later the visit; yet a meaningful share were already overdue when they were seen.



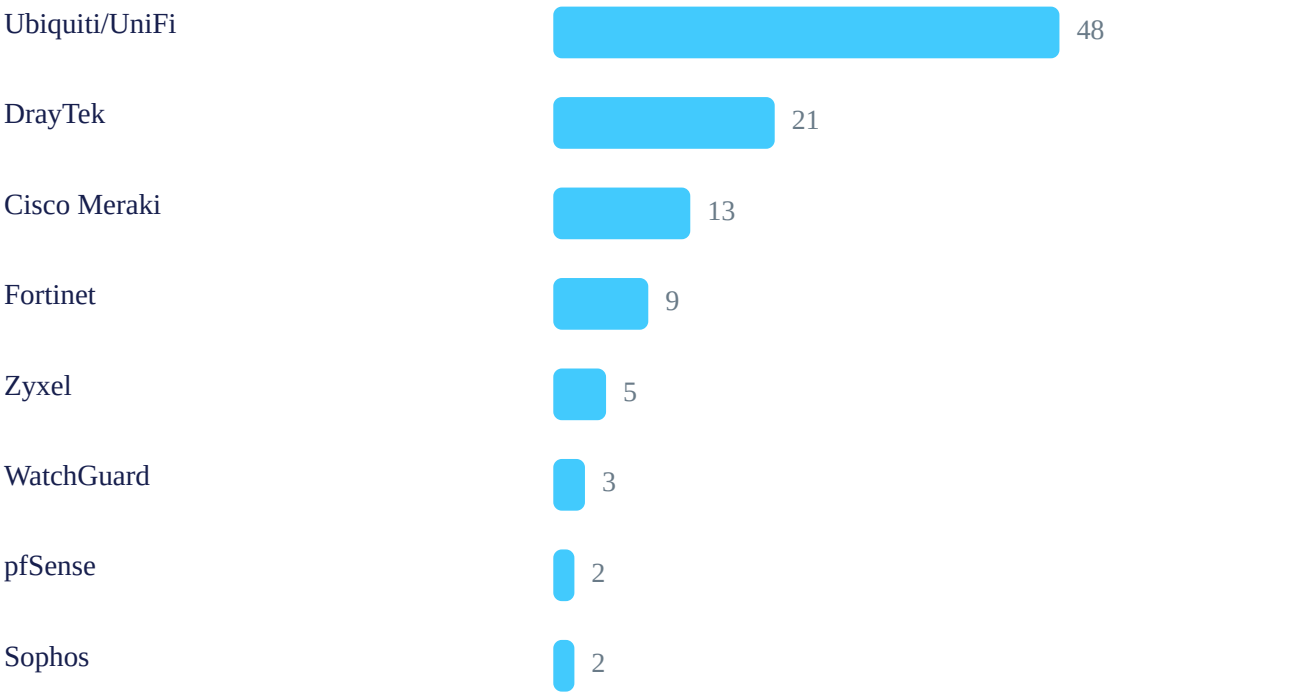
And often there was no real server at all. In about 29% of detailed audits the “server” was a desktop PC pressed into service, a peer-to-peer workgroup, or simply absent: a single ordinary computer quietly acting as the spine of the whole practice, with the resilience to match.

04 Security & resilience

The perimeter is, encouragingly, often the strongest area: where firewall or network hardware was identified, it was usually a proper business-grade device. **Ubiquiti/UniFi** dominates, followed by DrayTek, Cisco Meraki and Fortinet.

BUSINESS NETWORK HARDWARE: PRACTICES MENTIONING EACH MAKE

SOME USE MORE THAN ONE



THE SOFT UNDERBELLY: ACCESS & BACKUPS

Behind that hardware, habits were looser. **Generic shared logins and weak passwords** were flagged in 25% of detailed audits: staff sharing one account, the same password on every machine, kit left permanently logged in. The most consequential finding, though, was backups: in **17%** the backup was failing, partial or absent. The next section is where those numbers come to life.

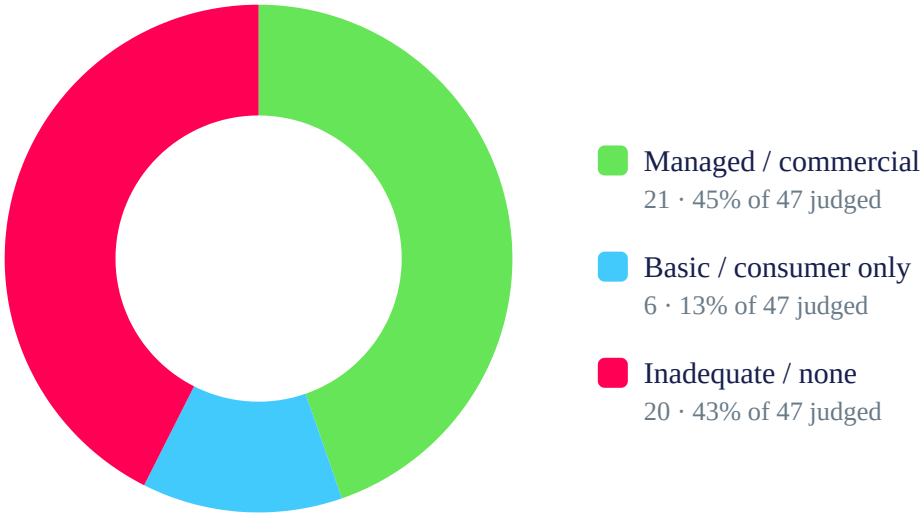
ANTIVIRUS: ONLY VISIBLE IN A QUARTER OF SITES

Antivirus is the one area where the audits themselves are thin. Most simply printed the checklist line *“Anti-virus software:”* and moved on, so for the large majority of practices there is **not enough recorded to judge** what was installed. Antivirus could be assessed with any confidence in just **47 of the 184 practices** (about a quarter); the rest are a genuine blank rather than a clean bill of health.

Where it *could* be judged, the picture splits almost in half. Around **21** practices had a proper **managed or commercial product** actually in use, named in the notes: ESET, Sophos, Bitdefender, SentinelOne, Vipre or business-grade Malwarebytes. But a similar number were running **inadequate protection or none at all**: expired licences, free consumer tools treated by the auditor as “effectively no antivirus,” or an inconsistent mix left behind by a history of infections. A handful more were on basic consumer-grade tools such as Microsoft Defender or free AVG.

ANTIVIRUS, WHERE IT COULD BE JUDGED

47 PRACTICES ASSESSABLE

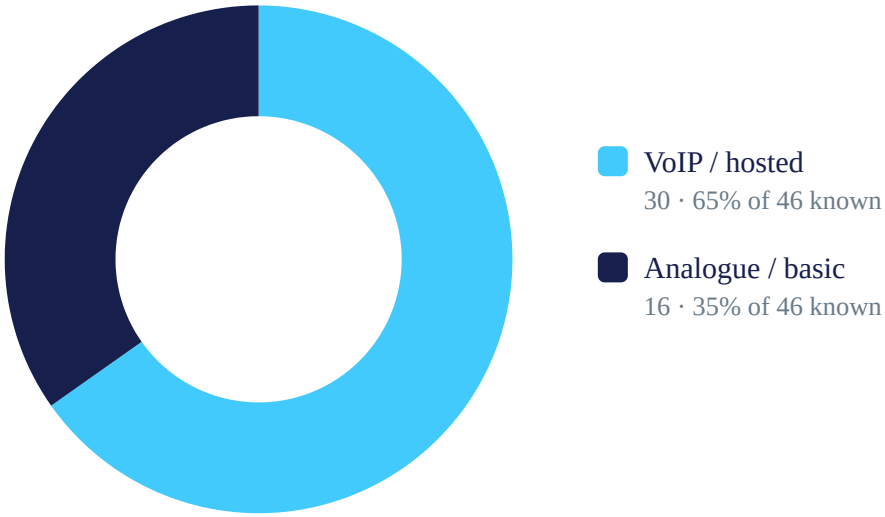


The takeaway is deliberately cautious: this is not “half of all practices had no antivirus.” It is that, in the minority of sites where an auditor actually recorded the antivirus in enough detail, a proper managed product was roughly as common as inadequate or absent protection, and everywhere else the honest answer is that the notes simply do not say.

TELEPHONY IN TRANSITION

PHONE SYSTEM

46 PRACTICES WHERE RECORDED



Telephony is mid-transition: most sites that had decided had moved to VoIP / hosted phones, but analogue lines persisted, and the move to VoIP was frequently bottlenecked by the very same slow broadband from Section 02.

05 Tales from the server cupboard

Numbers describe the estate; they don't quite convey what it feels like to walk into one of these rooms. These are real findings from the audits; the kind of thing that doesn't fit in a bar chart.

A note on names. Every practice below is given an **invented** name and every identifying detail removed. The aim is to learn from what happened, not to shame anyone; these are good clinics that trusted whoever set their systems up. Where a specific password is shown, it's included only because the weakness *is* the lesson. No real practice, person, address or domain appears here.

THE LIVE ONE

The practice that was being attacked while the engineer stood in the room

Call them **“Harbour Row Dental.”** During the on-site visit, the auditor found Remote Desktop (RDP) left open to the entire internet through the firewall: the digital equivalent of propping the back door open onto the street. The logs showed the practice was **under more or less constant attack**: a steady stream of break-in attempts only being “stopped” by the antivirus, which the report bluntly called a very poor idea, like leaving your front door unlocked and relying on a guard inside to tackle whoever wanders in.

There was no proper business firewall. Staff were reaching their desktops from home Macs using a mix of direct RDP, TeamViewer and a remote-access tool. The customer was **advised then and there, while the team was still on site,** to shut RDP down immediately and move to a VPN. RDP exposed to the internet remains one of the most common ways ransomware gets into small businesses; this one had been inviting it in for who knows how long.

LESSON · NEVER EXPOSE RDP TO THE INTERNET; USE A VPN, AND A FIREWALL THAT ISN’T THE ANTIVIRUS

THE TWO THAT HAD NEARLY EVERYTHING WRONG

When every layer fails at once

“Maple Bank Dental” was a clean sweep. The server lived *in the kitchen*. The cabling was a decade old and visibly a mess, with no comms cabinet. DNS was broken in three different ways across the network (some machines using the router, some external, some the server), and several PCs weren’t on the domain at all. A few copies of Windows weren’t even properly licensed. The antivirus had been *bought second-hand off eBay.* The house password was `Pa$$word`. And all of this ran over a connection measured at **under 2 Mbps**.

“Elm Court Dental” was its twin. Every member of staff logged in with the same password: `Password1!`. Every user was a full administrator, there was no network firewall, no multi-factor anything, the directory server appeared unlicensed, and the auditor could find no backup system at all. A single internet line with no failover completed the picture: one cut cable from total standstill.

LESSON · PROBLEMS COMPOUND; FIXING ONE LAYER BARELY HELPS WHEN THE OTHER FIVE ARE OPEN

THE PASSWORD HALL OF SHAME

“Everyone just uses the same one”

Beyond the two above, shared and guessable passwords were the rule rather than the exception. A representative sample, anonymised but otherwise exactly as found:

- **“Castlegate Dental”** ran a proper domain and then undid it: every account was generic, on the usual house password `Buffalo1`. The owner was sure there was an off-site backup, too; the auditor looked and couldn’t find one.
- At **“Bridge Street Dental,”** the BT router password was simply *handed out to patients*; with no separate guest Wi-Fi, visitors sat on the same network as the patient records. The same site was still running a Windows XP machine behind nothing more than that BT router.
- Across dozens of sites the note was the same: *“generic accounts, same password everywhere.”* When everyone is the same user, you lose any record of who did what, and one phished password opens the whole building.

LESSON · INDIVIDUAL ACCOUNTS, REAL PASSWORDS, MFA, AND A GUEST NETWORK THAT ISN’T THE CLINICAL ONE

NO FRONT DOOR

The practices with no firewall at all

A surprising number of sites had **no perimeter firewall whatsoever**: just the ISP’s router between the open internet and the patient records. The most striking, **“Granite City Dental,”** was even connected to an NHS national network: no firewall, just a basic router and a little VPN box bridging to the health service. Others were a standard BT or consumer router and nothing else. In security terms, the building had walls and a roof but no front door. And, as Harbour Row shows, the internet checks every handle.

LESSON · A BUSINESS-GRADE FIREWALL IS THE CHEAPEST INSURANCE A PRACTICE CAN BUY

THE ILLUSION OF SAFETY

The backups that ran perfectly every night and saved nothing

At **“Willowbank Dental,”** three different backup tools were installed on the server. The nightly job completed and logged itself as *done*; except the log, read closely, said the same thing every night: **errors: 2, processed files: 0, backed up files: 0, total size: 0 bytes.** For days on end the practice was faithfully, automatically backing up nothing at all, while everyone assumed they were covered.

At **“Northgate Dental,”** the cloud backup had been quietly throwing errors *since the previous April*, months of them, and the local backup to a network drive had stopped working too. Nobody knew until the auditor opened the logs. This is the recurring villain of the whole dataset: not dramatic failure, but the green tick that lies.

LESSON · AN UNTESTED BACKUP IS A GUESS; CHECK RESTORES, NOT JUST THAT THE JOB “RAN”

WHAT BACKUP?

When there was nothing to fail in the first place

Worse than a broken backup is no backup. The audit notes are sometimes just two words long: **“No backup here”** at one practice; *“no backup system confirmed: severe risk”* at another. Elsewhere the safety net was a single external hard drive dangling off the server that, on inspection, hadn’t been writing anything for a long time, or a drawer of assorted USB drives that no one could vouch for. A practice running entirely on one server with no copy anywhere is one failed disk, one fire, or one ransomware email from losing its patient records permanently.

LESSON · THE RULE OF THREE (THREE COPIES, TWO MEDIA, ONE OFF-SITE) EXISTS FOR A REASON

THE ONE THEY WERE WARNED ABOUT

A data loss foretold, in writing, months earlier

“Beechwood Dental” lost data. The painful part: their IT provider had spelled out the exact risk in an audit months before: that because the practice used generic accounts with files saved locally on individual PCs (not redirected to the backed-up server), data *could* be lost. For budget reasons the practice chose to carry on as-is rather than re-engineer the network.

Then a staff member opened a malicious email attachment that slipped past the mail filter, the firewall and the local antivirus, and the files that vanished were precisely the local, un-synced ones the report had flagged. The server data, which *was* backed up and monitored, came through fine. The difference between the data that survived and the data that didn’t was a network design decision made, and deferred, on paper.

LESSON · “IT’S ON THE SERVER, AND THE SERVER IS BACKED UP” ONLY WORKS IF FILES ACTUALLY LIVE ON THE SERVER

THE BROADBAND TIME MACHINE

Running 2025 software on a 2009 connection

Some sites were trying to run cloud practice-management software, card payments and digital imaging over connections that belonged to another decade. **“Riverside Orthodontics”** was measured at **2.7 Mbps down, 0.6 up**; for good measure, it had no firewall either. Another practice clocked an ADSL line synced at 8 Mbps down and barely half a megabit up, actually achieving under 4. A third was running on roughly **1 Mbps of upload** for the entire building. When a single X-ray can be tens of megabytes and the practice software lives in the cloud, this isn’t slow; it’s a daily tax on every appointment.

LESSON · CONNECTIVITY IS CLINICAL INFRASTRUCTURE NOW, NOT AN OVERHEAD TO MINIMISE

HELD TOGETHER WITH HOPE

The kit that should have retired years ago

Plenty of practices were running on hardware well past its dignity. One server was **“painfully slow to operate and almost unusable,”** in the auditor’s words. Several still ran **Windows Server 2008 or even 2003**; one note simply said it “should not be running on the network at all.” Workstations of **ten and twelve years old** were still in daily clinical use; one set were decade-old machines that had, at least, been well specified once upon a time. None of this fails dramatically, until the day it does, usually mid-surgery, with no spare and no backup.

LESSON · PLAN REPLACEMENTS ON A CYCLE, BEFORE THE HARDWARE PLANS THEM FOR YOU

LIGHTNING ROUND

The physical reality behind the network diagram

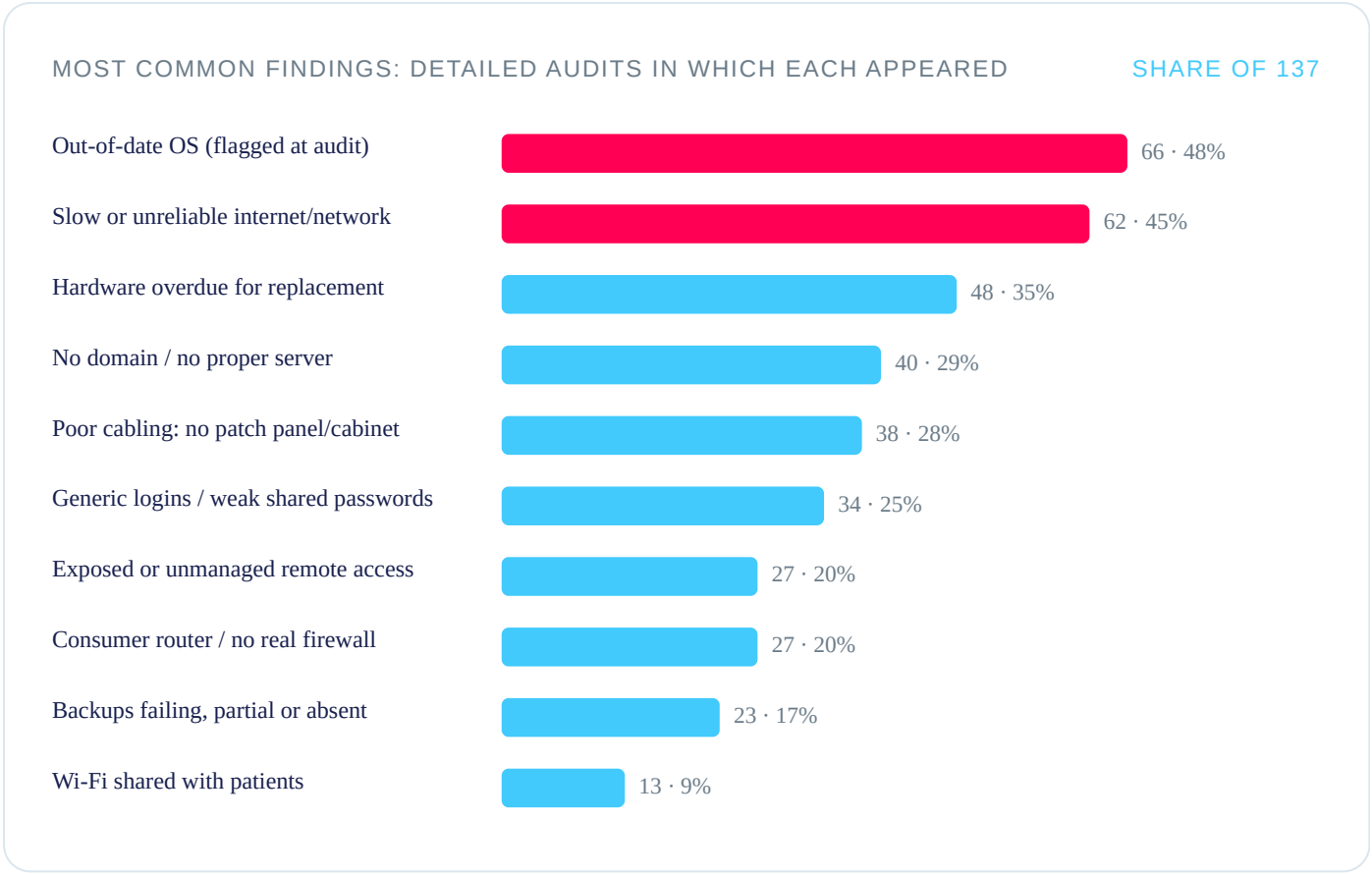
Not every find was a catastrophe; some were just the everyday physics of small-practice IT, collected here without comment:

- A patch panel sitting *on the floor* of the electrical cupboard, with PCs cabled off the back of a hinged cabinet door.
- A core switch tucked *under the stairs.*
- A server quietly relocated *into a cupboard*, ventilation optional.
- A “server” that turned out to be the *reception PC,* holding everyone’s files, with no redundancy of any kind.
- A CCTV system about *ten years old,* and a setup described only as *“ancient; all USB connections.”*
- And the simplest verdict in the entire archive: *“Very poor setup. Ancient.”*

LESSON · THE NETWORK IS ONLY AS RESILIENT AS THE CUPBOARD IT LIVES IN

06 The pattern across every site

Pulling the findings together, a consistent profile of the “typical” at-risk practice emerges. These are the issues that recurred most often across the 137 detailed audits:



Read top to bottom, it's the anatomy of small-business healthcare IT: **ageing software** and **performance pain** neck-and-neck at the top, then a cluster of **foundational weaknesses** (overdue kit, no domain, messy cabling, shared logins) that quietly cause the performance pain in the first place. The security gaps are fewer in number but, as Section 05 shows, by far the most expensive when they go wrong.

07 Field notes & caveats

A few honest limits on what this data can and can't tell you.

- **Depth varies hugely.** Some practices got a fifteen-page narrative; others a three-line note. Including the short ones is what gets us to 184 practices, but problem rates are quoted over the 137 audits with real detail; a thin note simply can't report a problem it never examined.
- **A multi-year snapshot, not a single moment.** These visits were carried out over at least five to seven years (roughly 2016–2025). Individual page timestamps are unreliable (many inherited a fixed "2017" template stamp), so a specific visit can't be dated precisely and no clean year-by-year trend can be drawn. Time-sensitive figures (speeds, OS currency) therefore mix eras and should be read in that light. What *is* reliable is that each auditor judged currency on the

day, so the “out of date / too slow” findings reflect genuine, contemporaneous shortfalls rather than hindsight.

- **Blank ≠ absent.** The checklist printed field labels (for things like RAID and UPS) whether or not they were filled in, so those items were excluded; counting the label would just count the template.
- **Under-counting, not over-counting.** Because unrecorded fields are common, the real prevalence of every problem above is most likely *higher* than shown.

Method & anonymisation

Source: 192 on-site IT audit documents covering 184 distinct practices (a handful of sites were audited more than once and have been merged). From a larger archive, clearly non-audit material was excluded: sales quotes and decks, internal staff/HR notes, blank templates, generic email proposals, a recruitment-agency survey and inbound enquiries. Each remaining document’s text was extracted and mined with keyword/pattern rules, then spot-checked by hand against the originals. Categorical fields (practice-management software, connection type, OS, firewall) are reliable; counts, speeds and antivirus depend on what each auditor chose to write down, and antivirus in particular was only recorded in enough detail to judge at about a quarter of practices. Every practice carries an internal anonymous ID only; no names, addresses, domains or other identifying details appear anywhere in this article, and every practice named in the stories is an invented pseudonym. Figures are estimates reconstructed from non-standardised source documents; broad-brush, and intended as such.

Prepared for Dental IT · 184 practices · 192 documents · all sites anonymised. Brand fonts: Apertura (primary, not web-embeddable) substituted with the brand’s Questrial alongside Montserrat.