

THE ELDEST GEEK · WHITE PAPER

The Doctor Family The Complete Story

Every competitor owns a column.
The Doctor Family owns the row.

The Eldest Geek · October 2026

Six benches, one family, one workflow. Five field doctors fix the machine in front of you — Windows, Mac, Linux, email — and the sixth, ServerDoctor, now runs the whole server: it finds the attack, tunes the box, cleans the hacked WordPress site, backs the server up to bare metal and hardens it.

This is the full story behind that claim: why the family exists, what each of the six doctors actually does, the headline expansion of ServerDoctor from a monitor into a six-job server bench, how the family compares category-by-category against the rest of the bench, who it's for, and what it costs. No single competitor spans it; each owns one column, and with ServerDoctor the row now reaches across nine paid-software categories that didn't apply a month ago.

MacDoctor 1.151 · WinDoctor 3.166 · LinuxDoctor 1.25 · EmailDoctor 1.12 · ServerDoctor 1.14

The pitch, in one page

Six benches, one family, one workflow — the tool diagnoses, decides, repairs and writes the paperwork, instead of just launching someone else's utility or reading a sensor.

Every bench problem has a dozen point tools. Hiren's and Medicat launch other people's utilities. HWiNFO reads a sensor. MXToolbox checks a record. Lynis prints an audit and hands you a to-do list. Each of them owns one column of the job and stops at the report. The Doctor Family was built the other way round: it **diagnoses, decides, repairs reversibly, and writes the case file** — across live Windows, docked drives, WinPE, macOS on Intel and Apple Silicon, any systemd Linux distro, any mail domain, and now the server itself.

Every Doctor prints a verdict a client can understand, saves a transcript, and drops it into a **case file** you can mail to a specialist — with a browser-readable `case.html` inside, no tooling needed on the other end. Run one doctor from the symptom menu, get the 10-second `--vitals` glance, let `--triage` rank everything into one do-these-in-order list, or run the whole **audit sweep** and walk out with the verdict table and the zip.

Honest by design. ServerDoctor and the field doctors are read-only by default. Every repair is consent-gated, validated before any restart, and reversible with a byte-exact undo. The tools never touch a file that isn't theirs, and they say *DO NOT REPLACE YET* or *offline* — *here are the manual steps* when that's the honest answer.

Licensing is a single self-serve 30-day trial — Ed25519-signed, verified offline. The five bench doctors share seats; ServerDoctor is licensed on its own, because after its 1.14 expansion it does a different and much larger job.

The six doctors at a glance

DOCTOR	PLATFORM	WHAT IT IS
MacDoctor 1.151	macOS (Intel + Apple Silicon)	The full Mac bench: 97+ checks, ~150 modes, one stick
WinDoctor 3.166	Windows 7 → 11, Server 2008 R2 → 2025	One signed .exe: 40 check groups, ~175 modes
LinuxDoctor 1.25	Any systemd distro	Log-autopsy + live diagnosis, native RAID/LVM recovery, carving, retained backups
EmailDoctor 1.12	Any mail domain	Deliverability & DNS-auth auditor that writes the fix
ServerDoctor 1.14	Linux (+ Windows) mail/web/app servers	Attack detection, perf tuning, WordPress security & forensics, bare-metal DR, host hardening

MacDoctor

MACOS · INTEL + APPLE SILICON

Mac rescue, OCLP unbrick, Fusion Drive rebuild, FileVault recovery, Photos migration and the full peripheral checkout — in one place.

WinDoctor

WINDOWS 7 → 11 & SERVER

The flagship and the broadest bench tool on the market: diagnose, decide, repair reversibly and write the case file across live Windows, docked drives, WinPE and Server.

LinuxDoctor

ANY SYSTEMD DISTRO

Capture-and-analyze-anywhere log autopsy plus native RAID/LVM recovery — the recovery engine that makes the "one family" claim true.

EmailDoctor

ANY MAIL DOMAIN

~25 deliverability checks across 8 DNS/transport groups — and it writes the DNS fix, where the monitors only check and alert.

ServerDoctor

LINUX (+ WINDOWS) SERVERS · THE STORY OF THE QUARTER

The server bench: attack detection, a 0–100 perf rating with applied tuning, WordPress security / forensics / incident response, bare-metal disaster recovery, host hardening, SSH 2FA and one-command installers — built from TEG-SENTINEL, SPAMDETECTIVE and PERFANALYZER.

The headline: ServerDoctor grew from a monitor into the whole server bench

1.0 → 1.14 — six jobs that used to mean six products and six bills, in one tool

In September, ServerDoctor watched a server. Now it runs one — read-only by default, every repair consent-gated and reversible.

Find the attack `--attack` · TEG-SENTINEL built in

- ▶ Brute-force, flood, port-scan, malware and C2 detection from the server's own logs, on Linux *and* Windows (Security log 4625/4771, IIS/Apache access logs, `netstat` / `ss`)
- ▶ A block ledger and firewall-aware teardown; `--block-ip` and `--harden` (xmlrpc, WordPress hardening) apply the countermeasure
- ▶ `--ftp` — distributed FTP brute-force defence: catches the slow, many-IP credential-stuffing pattern single-IP fail2ban rules miss, and orchestrates fail2ban to shut it down

Rate the box and tune it `--perf-snapshot` · `--perf-compare` · `--perf-fix` · `--tune`

- ▶ A calibrated **0–100 server rating** with fixed anchor points — a score means the same on every server and across weeks — plus a plain-English "how many WordPress/PHP sites can this host" verdict
- ▶ `--perf-fix` **applies** the tuning: InnoDB buffer pool sized to RAM, PHP-FPM `pm.max_children` from measured worker RSS, OPcache, a Redis object cache, swappiness, fstrim — reversibly, into drop-ins that never touch a file that isn't ours, validated before any restart, with a full undo
- ▶ `--tune` is the print-only audit: *is this box actually configured for the RAM and CPU it has?* — the classic field case being a 64 GB server still on the stock `innodb_buffer_pool_size=128M`

Fix the WordPress that's crawling `--wp-slow` · `--wp-overload` · `--wp-plugins`

- ▶ Runs wp-cli **as the site's own web user**, measures the full bootstrap against the core floor, and **bisects the active plugin list** to name the specific plugins costing the seconds — the synchronous licence-phone-home offenders — with the outbound URLs captured as the smoking gun
- ▶ `--wp-overload` answers "what's hammering it right now" — PHP-FPM pool saturation, xmlrpc / Action-Scheduler floods, a hung-request `max_execution_time`
- ▶ `--wp-plugins` classifies every plugin as used vs removable

Keep the server up and secure it

- ▶ `--2fa` — two-step SSH login (any TOTP app, or a FIDO2 hardware key) with a dead-man rollback so you can never lock yourself out; multi-distro, anti-lockout verified before every reload
- ▶ `--boot-check` — "after a power failure not all services come back": classifies each failed unit and offers systemd drop-ins, a boot watchdog and a byte-exact undo
- ▶ The diagnostic bench: `--web-outage` , `--vitals` , `--webpage` , `--storage` , `--certs` , `--backup-check` , `--updates` , `--exposure` , `--what-changed` , `--mailbox-check` , `--spam`
- ▶ One-command installers (menu group L): ISPConfig 3, Nextcloud, MongoDB and RAID tools + monitoring onto a fresh, preflighted server — official sources only, GPG-pinned, secrets shown once and never logged

New in 1.14 — the four that open whole new markets

- ▶ `--snapshot` — **WordPress site clone + backup**: a full copy of a site (files + database), pushed off-site over FTP or S3, on a schedule. The Duplicator / UpdraftPlus job, server-side
- ▶ `--wp-attack` — **compromised-site response**: a malware scan + forensic triage of a hacked WordPress install, ending in a **professional incident report (HTML/PDF)** you hand the customer or their insurer. The Wordfence / Sucuri / MalCare cleanup, with the paperwork
- ▶ `--backup` + `--harden-server` / `--secure-router` — **whole-server bare-metal disaster recovery**: image the entire server and restore it to a bootable restore USB, including to *dissimilar hardware*; plus multi-distro host hardening and the option to turn a server into a hardened router. The Clonezilla / ReaR / Veeam + Lynis / CIS job, in the tool that already found the attack

WinDoctor: new repair modes

Everything from September still ships. Added since:

- ▶ `--vcredist-fix` / `--msi-source` — the dreaded "the feature you are trying to use is on a network resource that is unavailable" dialog, usually a Visual C++ Redistributable whose cached MSI a disk-cleaner deleted (MSI source-resiliency loss). WinDoctor names the product whose source is gone and, behind a typed REPAIR consent, downloads the official Microsoft redist (aka.ms permalink, Authenticode-verified) and re-caches it; offline it prints the exact manual steps. Read-only until consent
- ▶ `--make-boot-usb` — the WinPE rescue stick now builds on sticks over 32 GB (big-stick FAT32 relayout), carries Intel VMD + AMD RAID drivers so it sees NVMe on modern boards, ships Memtest86+ on the UEFI boot menu, and dual-boots BIOS + UEFI; `--boot-usb-drivers` audits what's baked in
- ▶ `--winre-fix` — the KB5034441 `0x80070643` failure: the WinRE recovery partition is too small, resized consent-gated (reagentc + diskpart)

- ▶ `--bad-update` — rollback doctor with an updatable known-bad-KB knowledge base

- ▶ `--lag-doctor` — "why does this PC feel slow": ranks the real cause (SSD latency with an optional micro-benchmark, heat, runaway processes, GPU, power mode, battery, TRIM, free space, Surface firmware) and offers each fix

- ▶ `--raid-doctor` — a degraded hardware/RST RAID 1: names the drive to replace and the drive to keep by serial, cross-checked against the controller, SMART and RST metadata, or says DO NOT REPLACE YET. Read-only apart from an optional bay-LED locate; `--verify` after the swap

- ▶ `--enable-admin` / `--boot-to-cmd` — offline lockout recovery on a docked Windows: enable the built-in Administrator by RID 500, or set the next boot to a SYSTEM command prompt — no password cracking, no file swaps, reversible with `--restore`

- ▶ `--https-doctor` , `--disk-usage` / `--cpu-usage` , `--oobe-doctor` , the search doctor, `--migrate-windows-old` (Windows.old migration) and the Mark-of-the-Web doctor

"It says 100%" and "it just spins": the three hang doctors

- ▶ **Disk 100%** (`--disk-usage`) names the processes moving the bytes and walks the usual suspects: SysMain on a platter, the indexer, two antivirus products inspecting each other, the StorAHCI MSI-mode bug, TRIM off, free space under 10%

- ▶ **CPU 100%** (`--cpu-usage`) reads interrupt/DPC time for a driver storm, the clock against the rated max (a throttled CPU reads 100% because it's slow), and names unsigned burners

- ▶ **The beachball** (MacDoctor `--beachball`) reads the `.hang` reports macOS files itself, the uninterruptible waits, dead network shares, heat, snapshots, kexts and the OpenCore root patches

What each doctor actually does

Grouped by job, drawn from the capability sheet. Claims here are limited to what the tools ship today.

WinDoctor

V3.166 · 40 CHECK GROUPS · ~175 MODES · ONE SIGNED .EXE

DIAGNOSE & TRIAGE

- ▶ 40 automated check groups across live Windows, docked drives, WinPE and Server (2008 R2 → 2025)
- ▶ The hang trio — disk 100%, CPU 100% — plus `--lag-doctor` ranking the real cause of "feels slow"
- ▶ `--https-doctor`, `--oobe-doctor`, the search doctor, the Mark-of-the-Web doctor

REPAIR, REVERSIBLY

- ▶ `--vcredist-fix` / `--msi-source` for the "unavailable network resource" dialog (Authenticode-verified official redistributable)
- ▶ `--winre-fix` (KB5034441 / 0x80070643), `--bad-update` rollback doctor
- ▶ `--hive-repair`, `--offline-servicing` and docked-drive dump analysis for a non-booting Windows
- ▶ Offline lockout recovery: `--enable-admin` (RID 500) / `--boot-to-cmd`, reversible with `--restore`

RECOVER & CLONE

- ▶ `--clone-system` bootable whole-disk clone, resized to fit, SSD-aligned, source never written
- ▶ `--backup` dated hardlinked grandfather-father-son snapshots; `--raid-recover`, `--nas-recover`, `--carve`, `--recover` wizard
- ▶ Offline NTFS recovery & forensics: `--mft-restore`, `--image`, `--browser-extract`, `--cred-carve` (offline DPAPI)

CERTIFY HARDWARE & BUILD THE STICK

- ▶ Memtest86+, `--disk-scan`, the WinPE sweep, `--benchmark` and `--disk-health` ("slow or old?" / "is the drive dying?")
- ▶ `--make-boot-usb`: sticks over 32 GB, Intel VMD + AMD RAID drivers, Memtest on the UEFI menu, BIOS + UEFI dual-boot; `--raid-doctor` names replace-vs-keep by serial

MacDoctor

V1.151 · 97+ CHECKS · ~150 MODES · INTEL + APPLE SILICON

DIAGNOSE & TRIAGE

- ▶ 97+ automated checks and the full peripheral checkout in one stick
- ▶ `--beachball` reads the `.hang` reports macOS files itself — uninterruptible waits, dead shares, heat, snapshots, kexts, OpenCore root patches

RESCUE, UNBRICK & MIGRATE

- ▶ Mac rescue and OCLP unbrick; Photos migration
- ▶ `--fusion-rebuild` Fusion Drive rebuild; `--unlock` FileVault recovery — self-contained AES-XTS, self-checked against the filesystem magic so a wrong key is rejected, not emitted as garbage

RECOVER & CLONE

- ▶ `--clone-system` bootable whole-disk clone (Apple + Linux partitions, boots straight from USB)
- ▶ `--backup` retained snapshots; the shared recovery engine (`--raid-recover` , `--carve` , `--recover`)

LinuxDoctor

V1.25 · ANY SYSTEMD DISTRO · CAPTURE-AND-ANALYZE-ANYWHERE

LOG AUTOPSY & LIVE DIAGNOSIS

- ▶ Cross-distro engine: capture on the patient, analyze anywhere; live diagnosis + log autopsy

NATIVE RECOVERY

- ▶ Native RAID/LVM recovery: assemble mdadm 0/1/5/6/10 (incl. degraded, RAID 6 double-fault), Synology SHR / QNAP / Asustor, Areca-by-analysis
- ▶ Multi-filesystem signature carving (`--carve`) and retained hardlinked backups

EmailDoctor

V1.12 · ANY MAIL DOMAIN · ~25 CHECKS ACROSS 8 GROUPS

AUDIT & REMEDIATE

- ▶ ~25 deliverability checks across 8 DNS/transport groups (SPF, DKIM, DMARC and transport auth)
- ▶ Audits **and writes the DNS fix** with one-command remediation — where MXToolbox and GlockApps check and monitor but leave you to fix
- ▶ Prints a verdict a client understands and drops it into the shared case file

ServerDoctor

V1.14 · LINUX (+ WINDOWS) · SIX-JOB SERVER BENCH · READ-ONLY BY DEFAULT

FIND THE ATTACK

- ▶ `--attack` brute-force / flood / scan / malware / C2 detection from the server's own logs; `--ftp` distributed FTP defence; `--block-ip` + `--harden`

RATE & TUNE

- ▶ `--perf-snapshot` / `--perf-compare` 0–100 rating + "how many sites it can host"; `--perf-fix` applies resource- & co-service-aware tuning reversibly; `--tune` print-only audit

WORDPRESS SECURITY, FORENSICS & PERFORMANCE

- ▶ `--wp-slow` / `--wp-overload` / `--wp-plugins` name the slow plugin and the flood; `--wp-attack` malware scan + forensic triage + professional HTML/PDF incident report; `--snapshot` full clone off-site to FTP/S3, scheduled

KEEP IT UP, SECURE IT, RECOVER IT

- ▶ `--2fa` SSH two-step with dead-man rollback; `--boot-check` failed-unit classifier; `--harden-server` / `--secure-router` multi-distro hardening
- ▶ `--backup` whole-server image + bootable restore USB, restore to dissimilar hardware
- ▶ The diagnostic bench (`--web-outage` , `--certs` , `--exposure` , `--what-changed` , `--spam` ...) and one-command ISPConfig / Nextcloud / MongoDB / RAID installers

The shared bench, everywhere. Esc leaves a test cleanly with the findings still written; --vitals, --triage, case files, the offline fleet dashboard, IDENTIFY (--unit) and "A = yes to all" work the same way in every doctor.

HOW IT COMPARES

ServerDoctor vs the server stack

The nine categories that didn't apply in September. One tool replaces the lot.

Host hardening & server performance

CAPABILITY	LYNIS / CIS-CAT / ANSIBLE	MYSQLTUNER / HOST DASHBOARDS	SERVERDOCTOR
Audit the box against best practice	✓ (Lynis, CIS-CAT)	~ DB only (MySQLTuner)	✓
Apply the hardening, reversibly	X report only	X advice only	✓
0–100 server rating + "how many sites it can host"	X	~ partial	✓
Resource- & co-service-aware tuning (never starve PHP/Redis)	X	X blind to co-residents	✓
Validate + undo on every applied change	n/a	n/a	✓
Turn a server into a hardened router	X DIY	X	✓

Attack detection & brute-force defence

CAPABILITY	FAIL2BAN / CSF-LFD	WORDFENCE / SUCURI (NETWORK)	SERVERDOCTOR
Brute-force / flood / scan / C2 detection from the server's own logs	~ DIY rules	~ per-site	✓
Distributed FTP brute-force (slow, many-IP) caught	X single-IP rules miss it	X	✓ --ftp
Orchestrates fail2ban / blocks the IP for you	~ you configure it	X	✓
Works on Linux and Windows servers	X Linux only	~ app layer	✓

WordPress security, forensics, migration & performance

CAPABILITY	WORDFENCE / SUCURI / MALCARE / PATCHSTACK	DUPLICATOR / UPDRAFTPLUS	SERVERDOCTOR
Malware scan across every tenant from the server	~ per-site subscription + plugin	X	✓
Compromised-site forensic triage	~ paid IR add-on	X	✓ --wp-attack
Professional HTML/PDF incident report	~ Sucuri/Wordfence paid response	X	✓
Name the slow plugin by bisecting the active list	X	X	✓ --wp-slow
Diagnose "what's hammering the site right now"	~ partial	X	✓ --wp-overload
Full site clone + off-site FTP/S3, scheduled	X	✓ per-site plugin	✓ --snapshot
No plugin, no per-site subscription	X paid per site, per year	X per-site	✓ server-side

Bare-metal disaster recovery & lockout-safe access

CAPABILITY	CLONEZILLA / REAR	ACRONIS / VEEAM	SERVERDOCTOR
Whole-server image for disaster recovery	✓ manual / DIY	✓ enterprise-priced	✓ --backup
Bootable restore USB	~ (ReaR)	✓	✓
Restore to dissimilar hardware	~ (ReaR, expert)	✓ paid tier	✓
No per-workload licence	✓ free but DIY	X per workload	✓
SSH 2FA (TOTP or FIDO2) with dead-man rollback	X	X	✓ --2fa
One-command ISPConfig / Nextcloud / MongoDB / RAID installers	X	X	✓

✓ full · ~ partial / with caveats · X not offered. ServerDoctor is read-only by default; every repair is consent-gated and reversible.

The bench Doctors vs the rest of the bench

Windows · Mac · Linux. Each competitor owns a column; we own the workflow.

JOB	WHO'S STRONG THERE	WHERE WE STAND
Hardware certification & warranty codes	PC-Doctor (OEM codes)	Live-hardware test + SMART surface scan + WinPE sweep + Memtest on the stick; keep PC-Doctor for the RMA form
Bootable cloning	Macrium, EaseUS, AOMEI, Acronis	--clone-system: whole-disk, resized, Apple + Linux partitions, Server, in the tool that also diagnoses
Scheduled retained backups	Macrium, Acronis, Veeam Agent	--backup: dated hardlinked GFS snapshots on the OS's own copy tools
Deep data / RAID recovery	R-Studio, DMDE, UFS Explorer	--raid-recover (mdadm 0/1/5/6/10, degraded) + --carve multi-filesystem
Failed-NAS recovery	R-Studio, UFS Explorer, DiskInternals	--nas-recover (Synology SHR / QNAP / Asustor); --areca-recover by analysis
Component benchmarks	PassMark, AIDA64, HWiNFO	--benchmark: repeatable score + self-trend + the storage-class call
All-on-one-stick toolkits	Hiren's, Mediat	They launch other people's tools; we diagnose, decide and write the case file
FileVault / encrypted recovery	Passware, ElcomSoft, Paragon	--unlock: AES-XTS decrypt with a known key, self-checked against the FS magic
Email deliverability	MXToolbox, GlockApps	EmailDoctor audits and writes the DNS fix; they check and monitor
Fleet / RMM	NinjaOne, Atera, Action1	Different class — always-on agents; our fleet is visit-history, run alongside an RMM

Capability matrix across the family

CAPABILITY	WIN	MAC	LINUX	EMAIL	SERVER
10-second vitals + ranked triage	✓	✓	✓	~	✓
Case file + browser-readable report	✓	✓	✓	✓	✓
Bootable whole-disk clone	✓	✓	~	✗	✗
Retained / bare-metal backup	✓	✓	✓	✗	✓
Deep data / RAID / NAS recovery	✓	✓	✓	✗	✗
Benchmark + "slow or old?" / drive health	✓	✓	~	✗	✓
Attack / brute-force detection	~	✗	~	✗	✓
Performance tuning, applied	✗	✗	✗	✗	✓
WordPress security / forensics / IR	✗	✗	✗	✗	✓
Deliverability / DNS-auth fix	✗	✗	✗	✓	~
Host hardening + SSH 2FA	✗	✗	✗	✗	✓

✓ full · ~ partial · ✗ not this doctor's job.

Who it's for

The bench doctors sell to anyone who fixes machines. After the 1.14 expansion, ServerDoctor's buyer is anyone who **operates** servers — and that's a bigger room.

MSPs

Attack-hunting, hardening, DR and WordPress incident response in one tool instead of stitching together Lynis + fail2ban + Veeam + Wordfence + Duplicator per client. The biggest new segment — run it alongside your RMM for the deep jobs the RMM doesn't do.

Web hosts & agencies

"How many sites can this box host" + applied tuning + scheduled off-site snapshots + compromised-site response is a hosting-ops suite. A host with 50 tenants paying per-site for Wordfence/Sucuri and per-workload for Veeam sees ServerDoctor collapse that into one licence.

WordPress shops & freelancers

--wp-slow / --wp-overload / --wp-plugins / --wp-attack / --snapshot is a full WP-ops toolkit that doesn't need a plugin or subscription on every site.

Repair shops

The field doctors are the one stick a Windows or Mac shop can't run the bench without — and ServerDoctor turns "we fix PCs" into "we also keep your server up, secure and backed up": a recurring-revenue service line, not a one-off repair.

Field techs

One signed .exe, one Mac stick, one Linux binary — capture-and-analyze-anywhere, read-only by default, every verdict a client can understand, and a case file you can mail to a specialist with a browser-readable report inside. EmailDoctor is the small, sharp upsell that attaches to every hosting and deliverability conversation ServerDoctor now starts.

What a buyer pays today to cover ServerDoctor's scope separately

CATEGORY	TYPICAL INCUMBENT SPEND (VERIFY CURRENT EDITIONS)
Host hardening / benchmark	Lynis Enterprise ~\$300+/yr, CIS-CAT membership
Perf tuning	MySQLTuner (free advice) + a consultant's time
Brute-force / flood defence	fail2ban / CSF (free) + setup labour
WordPress security / malware	Wordfence ~\$119, Sucuri ~\$200–300, MalCare ~\$99–149, Patchstack ~\$99 — per site, per year
WordPress forensics / IR	Sucuri / Wordfence response ~\$200–950 per incident/yr
WordPress migration / clone	Duplicator Pro ~\$99–549/yr, UpdraftPlus ~\$70–195/yr
Bare-metal DR / server backup	Acronis / Veeam ~\$ per workload/yr; ReaR / Clonezilla free but DIY
SSH 2FA	Duo ~\$3–9/user/mo

The economics in one line. A single hosted WordPress server covered "properly" with the incumbents — security + backup + migration — is easily **\$400–800/yr before labour**. ServerDoctor does all of it from one binary.

PRICING

What it costs

The bench Doctors

Technician

\$99/yr

\$199 lifetime

- One platform doctor, all modes
- Trial: self-serve 30 days
- Offline-verified licence

BEST VALUE

Cross-Platform Bench

\$149/yr

- Win + Mac + Linux + Email
- The full field bench
- One licence, every patient

Shop

\$299/yr

- Multi-seat for a shop
- Fleet dashboard + report store
- Priority support & tickets

Bench pricing is final. The five field doctors share seats; a self-serve 30-day trial is Ed25519-signed and verified offline.

NEW — Server & MSP licensing **NEW TIER**

ServerDoctor is licensed separately from the bench bundle. After 1.14 its scope spans nine paid software categories, so it carries its own three-rung ladder, priced per server, per year and anchored to "cheaper than

the stack it replaces."

Solo

\$249/yr · 1 server

- The whole server bench
- Cheaper than "Wordfence + a backup tool" on one box

FOR MSPS & HOSTS

MSP

\$899/yr · up to 10

- ~\$90/server
- Beats per-site WP security + per-workload DR across a fleet

Fleet

\$1,999/yr · 25+

- Volume tier for hosts
- Custom above 25 servers

Introductory / indicative pricing. The ServerDoctor Solo / MSP / Fleet numbers above are introductory and indicative, not final — they are anchored to the stack they replace (a single hosted WordPress server covered by the incumbents runs roughly \$400–800/yr before labour) and are subject to confirmation. Please ask for a current quote.

GET IT

One family, one workflow, the whole row

Diagnose, repair, recover, clone, benchmark — and now hunt the attack, tune the box, clean the hacked site, back the server up to bare metal and harden it. On Windows, Mac, Linux, email and the server itself, from one family.

Start the self-serve 30-day trial. One licence, every patient.

The Eldest Geek · theeldestgeek.com

Competitor capabilities and prices are drawn from the vendors' published documentation, October 2026 — **verify current editions** before quoting. Prices move quarterly; the capability columns are the durable comparison. The Doctor Family tools are read-only by default and every repair is consent-gated, validated and reversible.

The Eldest Geek · The Doctor Family · The Complete Story · October 2026. Versions: MacDoctor 1.151 · WinDoctor 3.166 · LinuxDoctor 1.25 · EmailDoctor 1.12 · ServerDoctor 1.14.