SECURITY
SOLVE

Security Solve

Protection for your devices, your networks and your remote team

Feature overview · November 2026

by TECHNOLOGY SOLVE

techsolve.io

OVERVIEW

Security for your whole business, in one app

Protection for your team's phones and PCs on any network, secure access to your offices, and whole-office filtering, managed by you and Technology Solve from one place.

Shield VPN
Encrypts every connection and blocks ads, trackers, malware and phishing, on any Wi-Fi.

Malware protection
Scans apps and downloads; flags fake updates, banking trojans and stalkerware.

Phishing protection
Blocks 1.8 million+ known phishing and malicious sites, and checks any link before you open it.

Live threat map
See every connection a device makes, where it goes, and what was blocked.

Remote office access
Reach office servers, remote desktop and file shares from anywhere, with no open ports.

Site-to-site links
Link your offices; choose exactly which machines can reach which.

Office IP, anywhere
Staff can browse from your office's internet address, for IP-restricted portals, still filtered.

Router gateways
Your pfSense, OPNsense or MikroTik can link the office: nothing to install on a PC.

Servers in your region
A private server in the region you choose: our cloud, or yours, such as AWS.

Company DNS
Internal names such as rds.company.local just work over the VPN.

Whole-office filtering
Point your router or firewall at Security Solve: every device in the office is protected.

Your rules
Block sites, whole categories or your own lists, and restrict devices that fall out of compliance.

Company portal
See your servers, offices and machines' health, your people and devices, and make changes yourself.

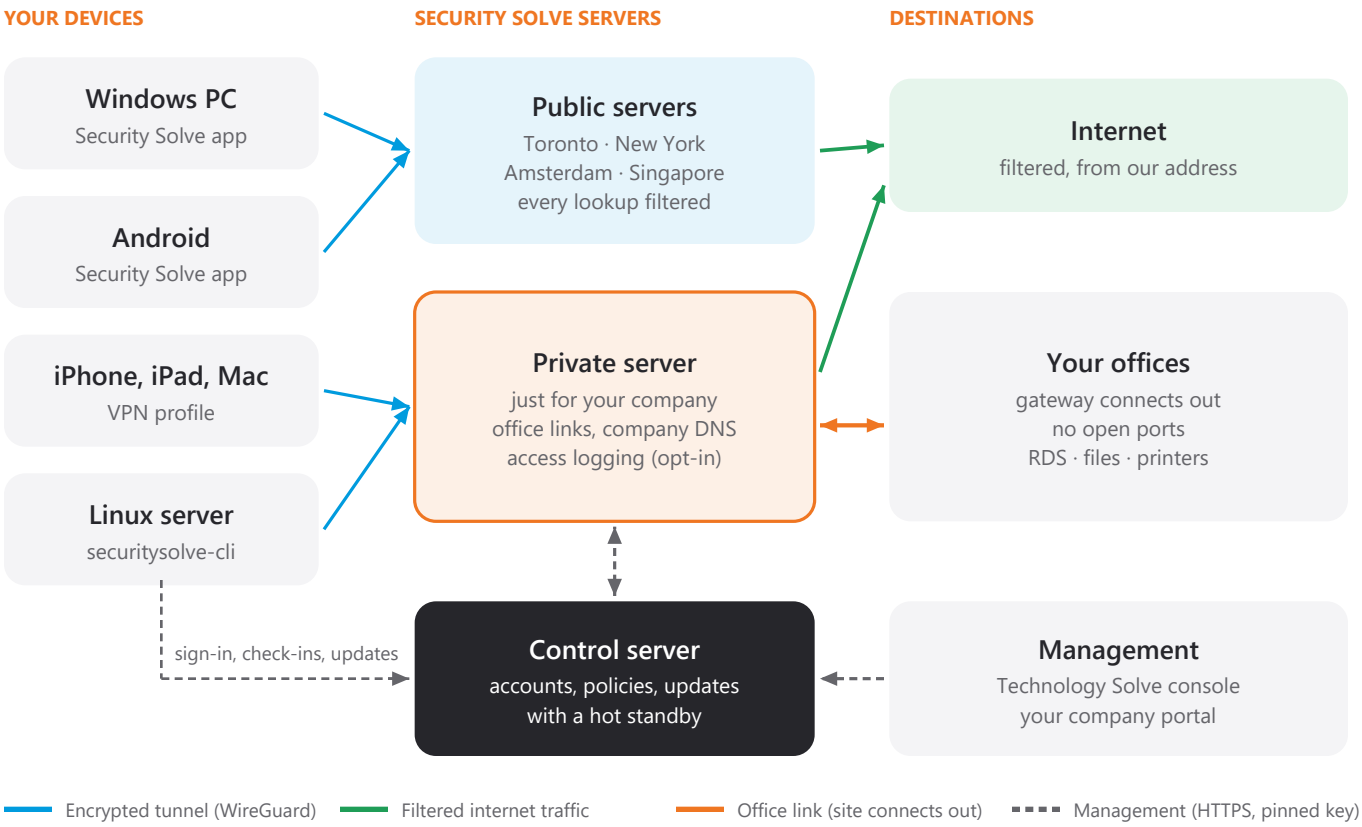
Private by design
No browsing logs. Optional access logging only on your own servers, and your people are told.

Managed for you
Technology Solve monitors, updates and supports everything.

THE BIG PICTURE

How it fits together

Your devices connect to Security Solve servers, which filter every lookup and reach your offices. A control server, with a standby ready to take over, keeps accounts, policies and updates in step.



- **Your devices** each have their own keys. Nothing is shared between devices or between companies.
- **Public servers** in four cities, or a **private server** just for your company, in the region you choose.
- **Your offices** connect out to your private server, so nothing at the office is exposed to the internet.

Works on

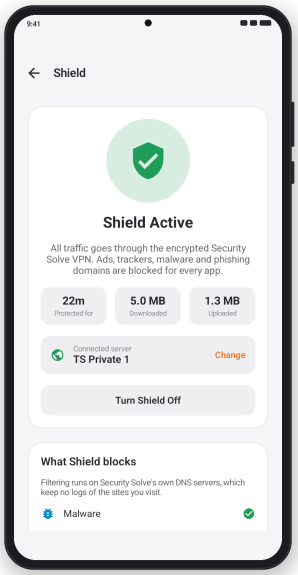
Device	How
Windows 10 / 11, Android	Security Solve app (Windows updates itself; Android from Google Play or direct download)
iPhone, iPad, Mac	Secure VPN profile for the free OpenVPN Connect app
Office gateways	Linux or Windows Server (securitysolve-cli), or your pfSense, OPNsense or MikroTik router; any router for whole-office filtering

PROTECTION

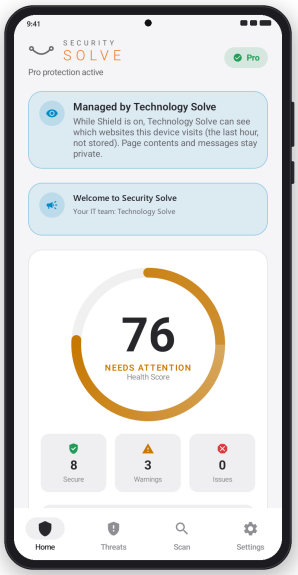
Shield: a VPN that blocks threats

One tap encrypts all of a device's internet traffic and filters it through Security Solve's own servers.

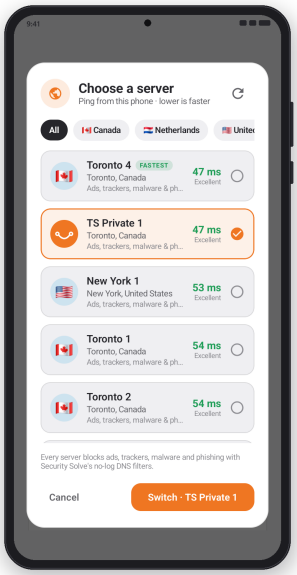
- **Encrypted everywhere:** hotel, airport and coffee-shop Wi-Fi can't see or tamper with your traffic.
- **Blocks threats for every app:** malware, phishing, ad and tracker sites are stopped before they load.
- **No logs:** our filtering servers keep no record of the sites you visit.
- **Fast servers**, picked by speed, or your company's private server. **Always on:** reconnects by itself after restarts and updates.



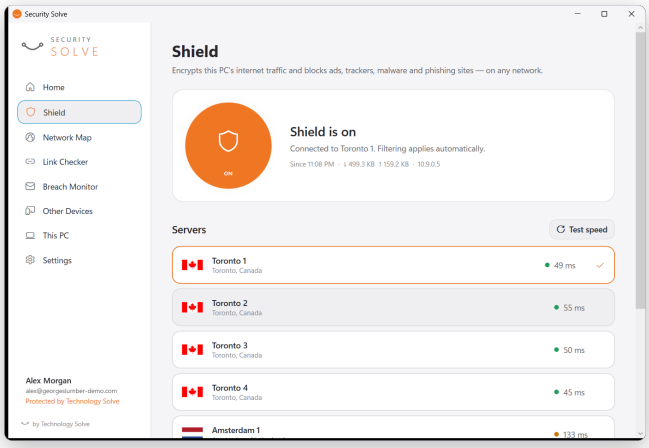
Shield on



Home: health score



Pick a server



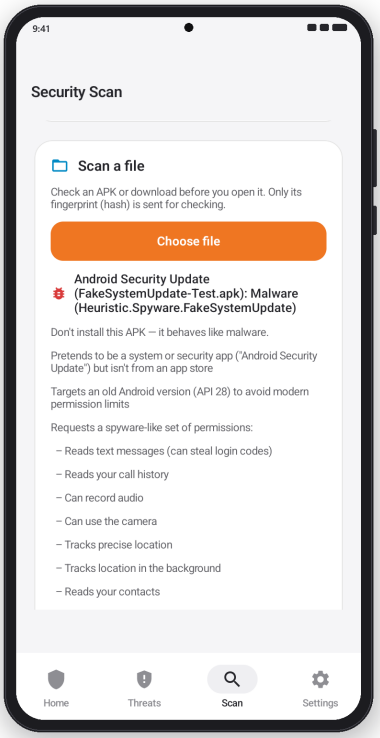
Security Solve for Windows: Shield

PROTECTION

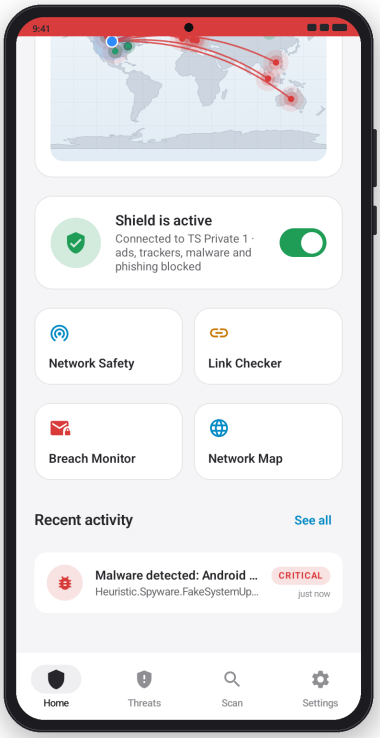
Malware protection

Security Solve checks every installed app and every APK you download against threat intelligence and its own behaviour checks.

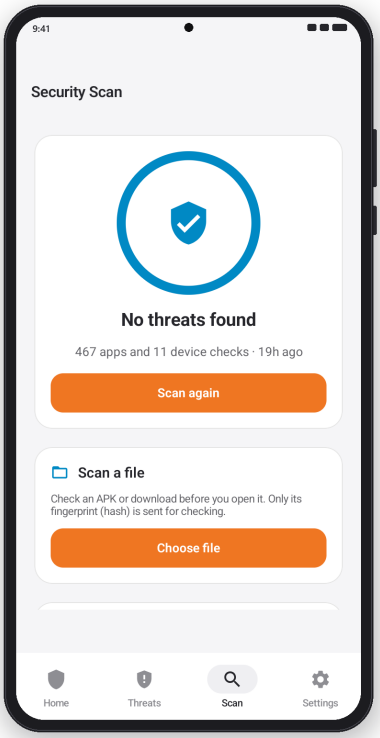
- **App scan** of everything installed, daily and on demand. **Real-time protection:** new installs are checked within seconds; dangerous ones raise an alert with Uninstall now.
- **Scan a file** before you open it. Only its fingerprint is sent for checking.
- Detects fake system updates, fake banking apps, banking trojans, stalkerware and spyware-like permission sets, from malware and stalkerware databases refreshed every 6 hours.
- Infected devices can be **quarantined automatically** until they're clean (see Your rules).



A test file flagged as spyware



Detections appear on Home

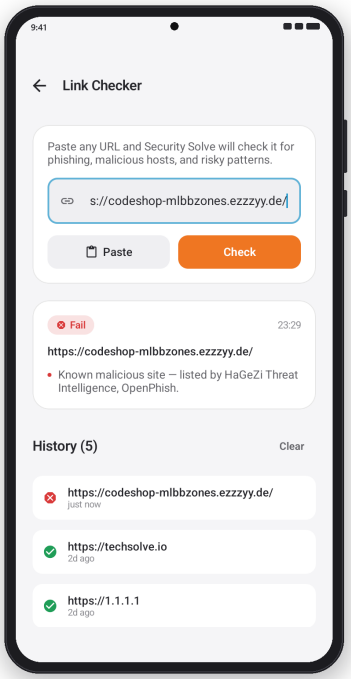


Full device scan

PROTECTION

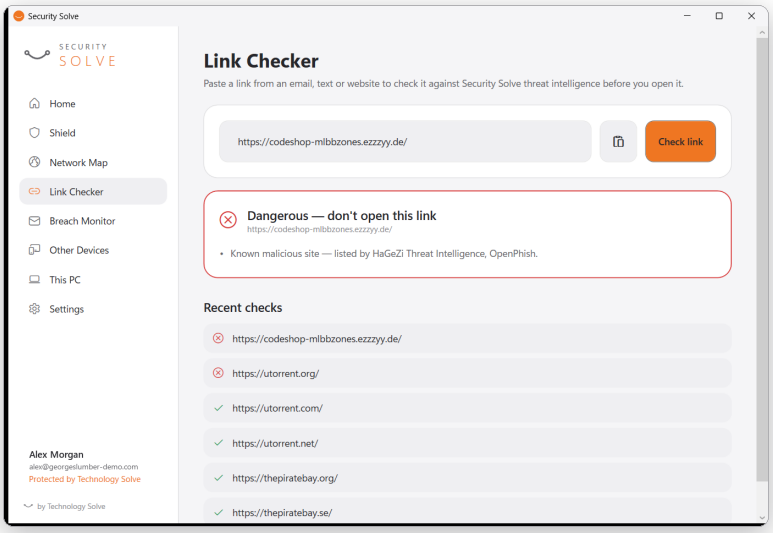
Phishing protection

Phishing sites are blocked the moment Shield is on, in every app and browser. The Link Checker answers "is this link safe?" before anyone clicks.



A live phishing link, flagged

- **1.8 million+** known phishing and malicious domains from OpenPhish, Phishing.Database and HaGeZi threat intelligence, refreshed every 6 hours.
- **Link Checker** on phone and PC: paste a link and get a clear verdict and the list that flagged it.
- **Share to Security Solve** from any Android app to check a link instantly.
- Blocked lookups show on the threat map and in your company's protection charts, so you can see attacks being stopped.

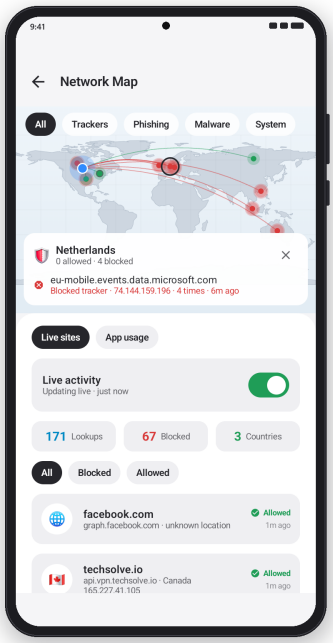


The same link on Windows: "Dangerous: don't open this link"

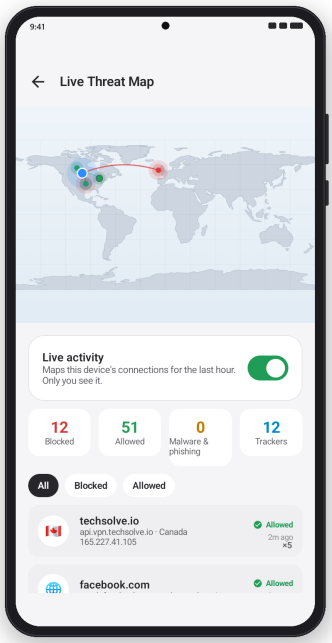
VISIBILITY

See what your devices connect to

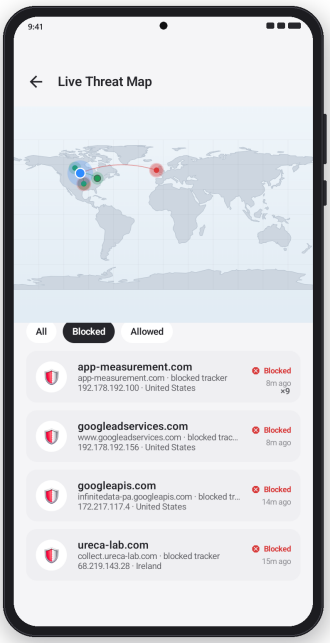
The Live Threat Map and Network Map show every connection from the last hour: where it went, which app or service, and what Shield blocked.



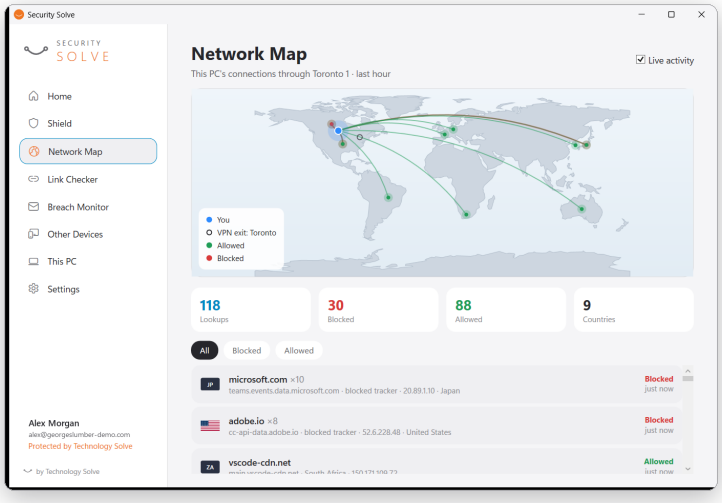
Network Map



Live Threat Map



Blocked trackers

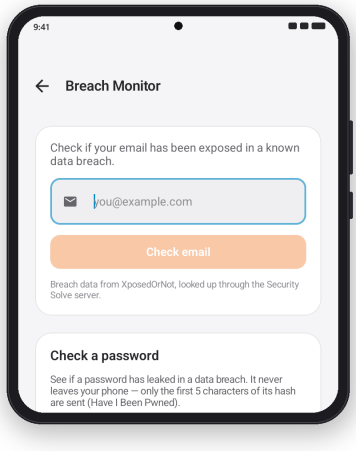


Network Map on Windows: 30 blocked lookups in the last hour

Activity stays on the device, kept in memory for one hour and never stored.

AWARENESS

Breaches, Wi-Fi safety and device health



Breach Monitor

Breach Monitor

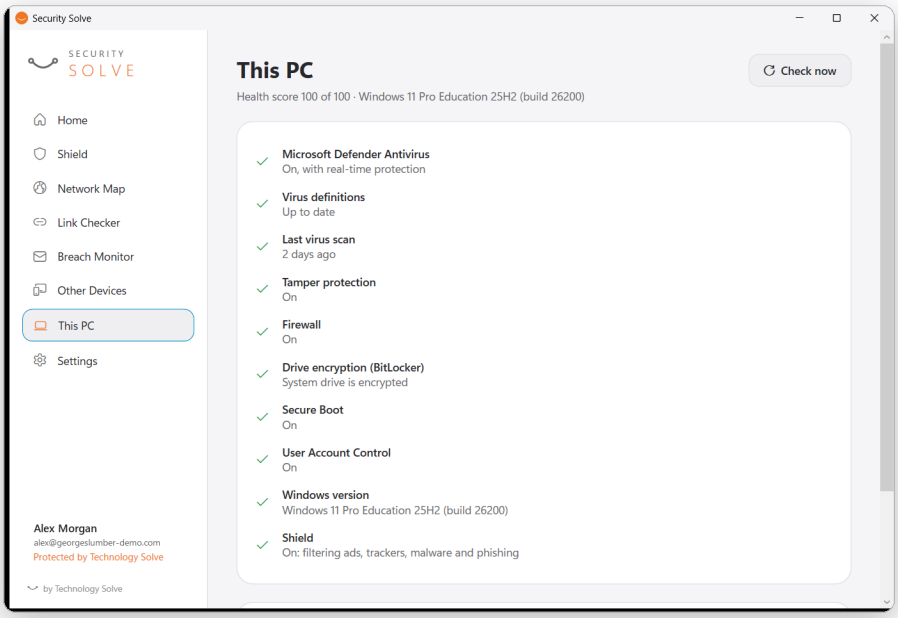
- Checks your email addresses against known data breaches and re-checks daily; alerts follow your account to every device.
- Check whether a password has leaked: it never leaves the device (only the first 5 characters of its hash are sent).

Network Safety

- Checks the Wi-Fi you're on: encryption, DNS hijacking, captive portals.
- Wi-Fi Guard warns on open or weak networks, with one-tap Turn on Shield.

Device health

Every device gets a health score from 0 to 100 (antivirus, encryption, firewall, updates, Secure Boot, screen lock and more), reported to your company portal so problems get fixed before they become incidents.

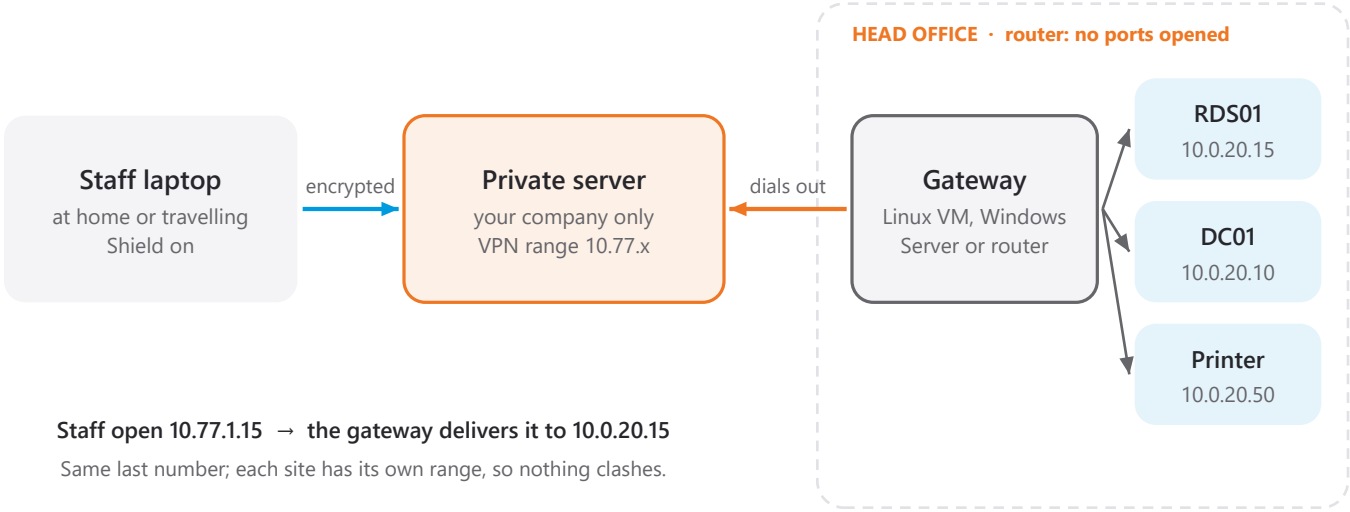


This PC: Defender, BitLocker, firewall, Secure Boot and more

REMOTE ACCESS

Your office, from anywhere

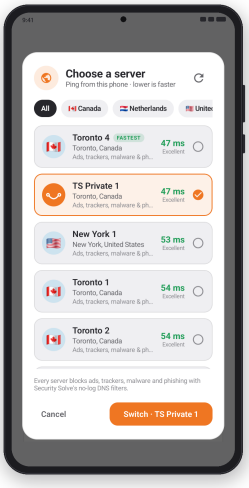
Replace your old remote-access VPN. Staff connect to your company's private Security Solve server and reach the office: remote desktop, file shares, printers and line-of-business apps.



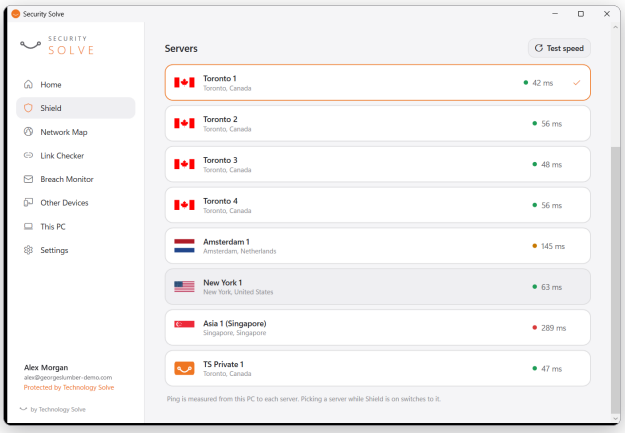
Staff open 10.77.1.15 → the gateway delivers it to 10.0.20.15

Same last number; each site has its own range, so nothing clashes.

- **Private server:** only the people and organisations you choose can see or use it. It shows with the Technology Solve smile in the app.
- **No open ports:** a small gateway at the office connects out: a Linux VM, an always-on PC, a Windows Server, or your pfSense, OPNsense or MikroTik router.
- **Still protected:** staff keep Shield's filtering for everything else they do.



Your private server in the app



And on Windows

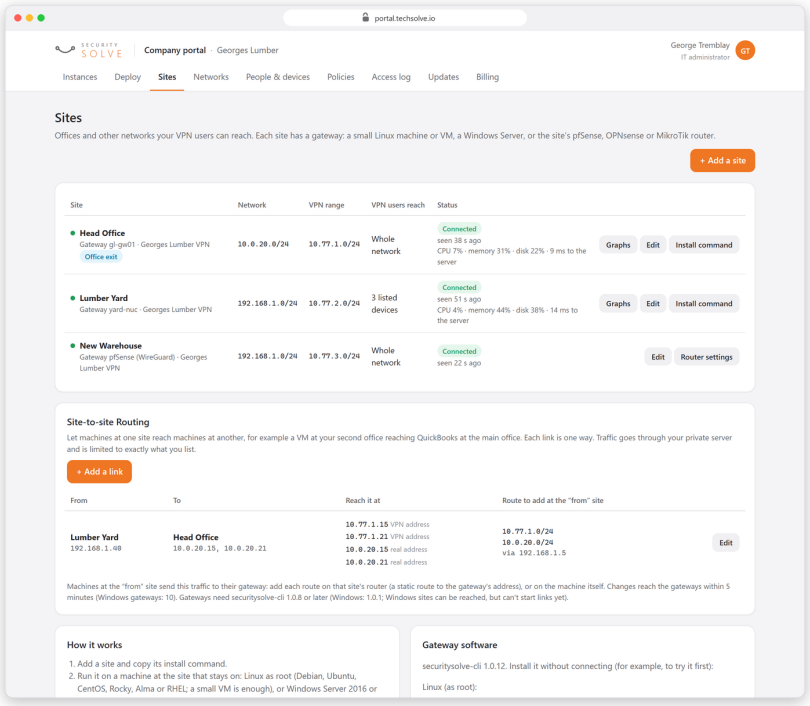
REMOTE ACCESS

Sites, routes and site-to-site links

Every office gets its own VPN address range, so offices can use the same internal addresses and nothing clashes with staff's home networks.

Site	Office network	Staff use	Example
Head Office	10.0.20.0/24	10.77.1.x	RDS01 at 10.0.20.15 is 10.77.1.15
Lumber Yard	192.168.1.0/24	10.77.2.x	Scale PC at 192.168.1.40 is 10.77.2.40
New Warehouse	192.168.1.0/24	10.77.3.x	Same LAN range as the yard, no clash

- **Whole network or listed devices:** give staff the whole office, or only the remote desktop server and the domain controller.
- **Site-to-site links:** let a machine at one office reach chosen machines at another (for example the yard's PC reaching the accounting server at head office), one way, exactly as listed.
- **Static routes:** give any machine its own VPN address. Changes apply in seconds and never need anyone on site.

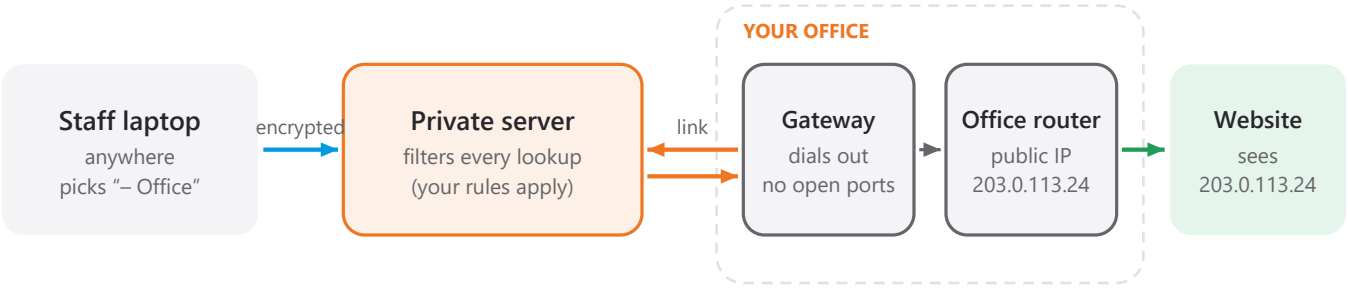


Company portal: your offices, their VPN ranges and gateway status

REMOTE ACCESS

Office Exit: your office's IP address, anywhere

Some banks, government portals, vendor sites and licence servers only let in your office's internet address. With Office Exit, staff working from home or on the road appear to come from the office.



Same protection as Shield, but websites see your office's address: for IP-restricted banking,

government and vendor portals. If the office link is down there's no internet, never another address.

- **Pick it in the app:** your private server gets a second entry, for example Private 1 – Head Office. Staff choose it when they need the office's address, and the normal entry the rest of the time.
- **Still protected:** every lookup is filtered exactly as with Shield: your block lists, categories and threat protection all apply.
- **Never the wrong address:** if the office's internet or gateway is down, people on the Office entry have no internet until it's back. Their traffic never quietly leaves from somewhere else.
- **Your choice:** turn it on for one office per private server in the company portal (Sites → Edit). Only your organisation's people see it.

Good to know. Office Exit traffic uses your office's internet connection, so speed depends on the office's upload speed, and your internet provider sees that traffic as coming from your office. Use it for the sites that need it, not as everyone's everyday connection.

NETWORKS

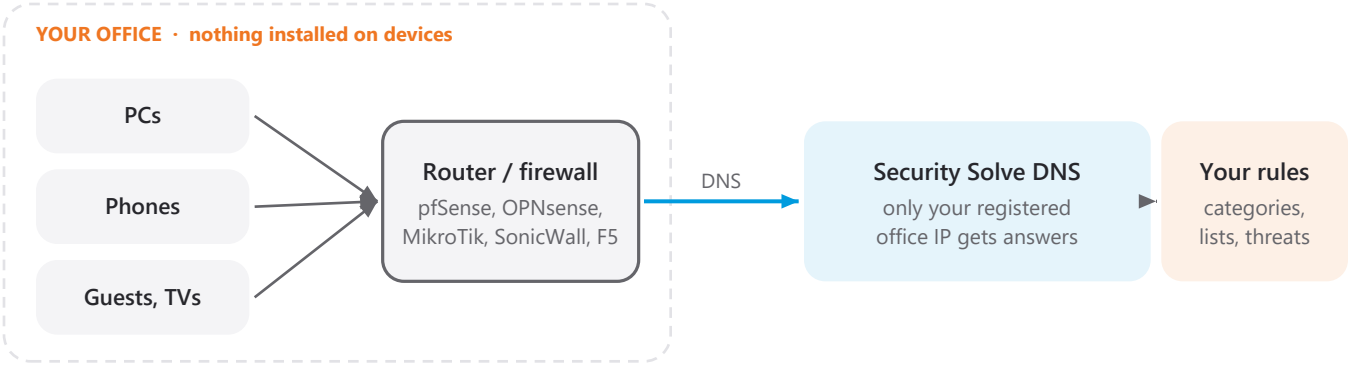
DNS that knows your company

Internal names like rds.georgeslumber.local work over the VPN exactly as they do in the office, so Remote Desktop, RD Gateway and file shares work by name.

- **Internal domains:** your domain controller answers for your company's names, through your office link.
- **Automatic translation:** office addresses in the answers become VPN addresses staff can reach. **Search domains:** type just rds, as in the office.
- **Choose your filtering** on your private server: Security Solve filtering, unfiltered (our own no-log resolver), or your own DNS servers. Your block lists apply in every mode.

Whole-office filtering through your router

Register your office's internet address in the company portal and point your router or firewall at Security Solve's network DNS. Every device in the office, including guests, TVs and anything that can't run an app, gets your company's filtering.



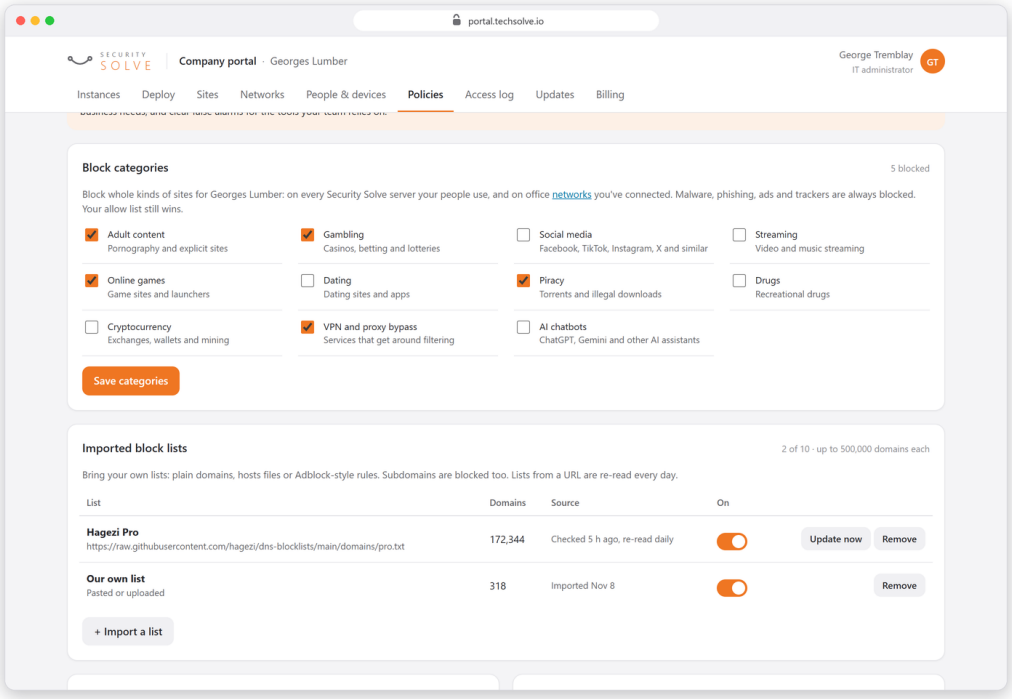
- Only your registered addresses get answers, so it's never an open resolver. Dynamic IP? The router updates it automatically.
- Step-by-step guides in the portal for pfSense, OPNsense, MikroTik, SonicWall and F5 BIG-IP.

CONTROL

Your rules: filters and device compliance

Decide what your devices can reach, and what happens when a device isn't healthy. Changes reach every server within a minute.

- **Block sites** for your organisation, indefinitely or for a set time; **always allow** the sites your business needs.
- **Block whole categories:** adult content, gambling, social media, streaming, online games, dating, piracy, drugs, cryptocurrency, VPN and proxy bypass, AI chatbots.
- **Bring your own lists:** paste, upload or link up to 10 block lists (hosts, Adblock or plain domain formats); linked lists refresh daily.



Company portal: block whole categories and import your own lists

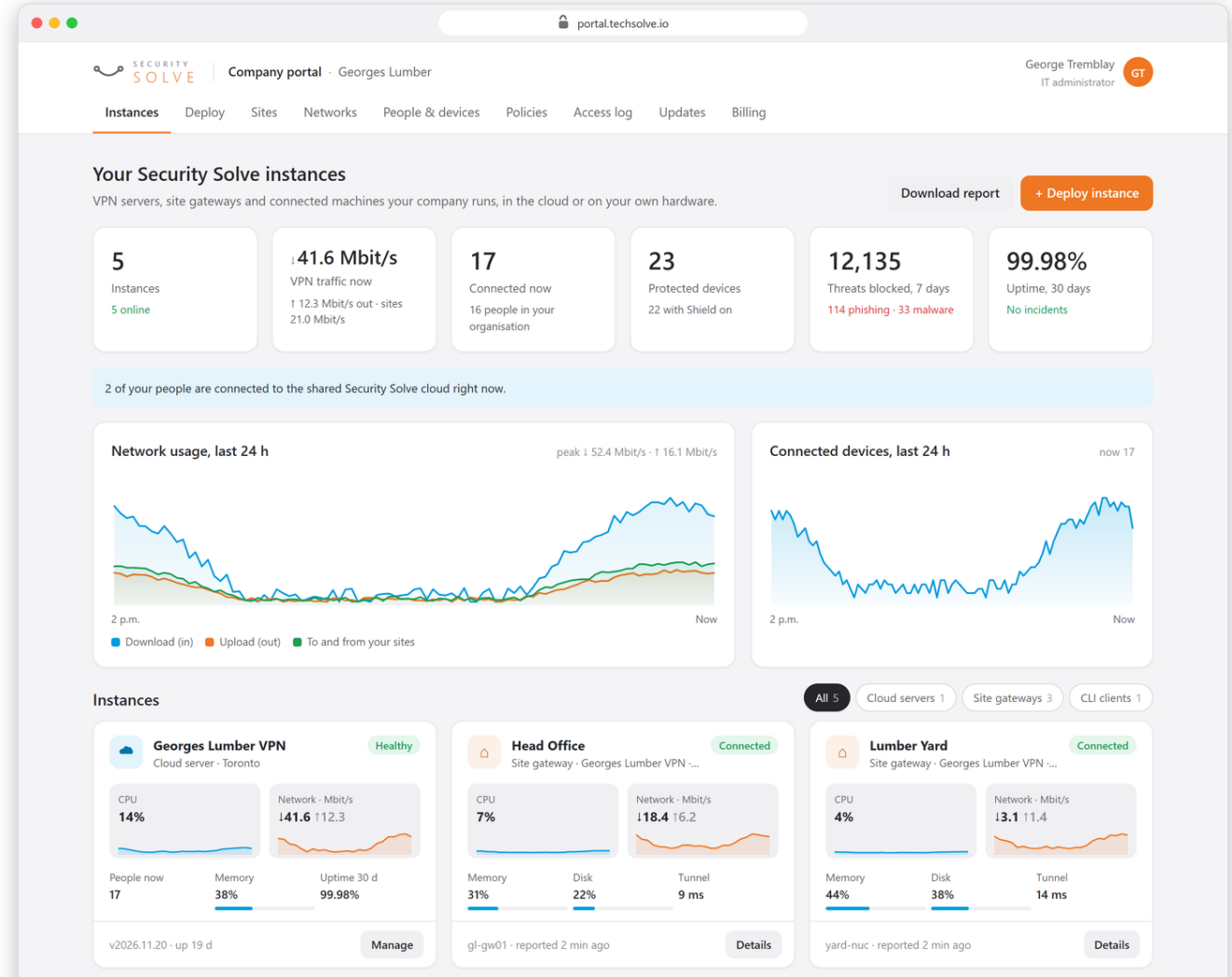
Device compliance (access policies)

- **Conditions:** minimum health score, no open threats, minimum app version, recent check-in.
- **Actions:** block chosen sites (for example Microsoft 365 on unhealthy devices), or quarantine the device until it's fixed. Users are told why, and how to fix it.

COMPANY PORTAL

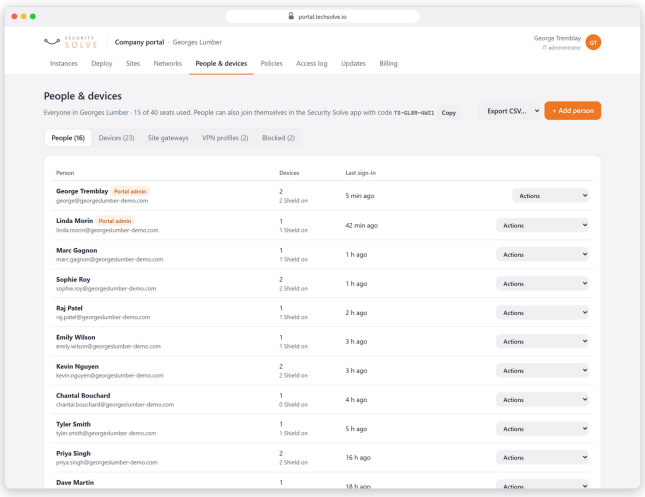
Your company's Security Solve, in one place

Your IT administrator signs in at portal.techsolve.io to see how Security Solve is protecting the company and make everyday changes without waiting for a support ticket.

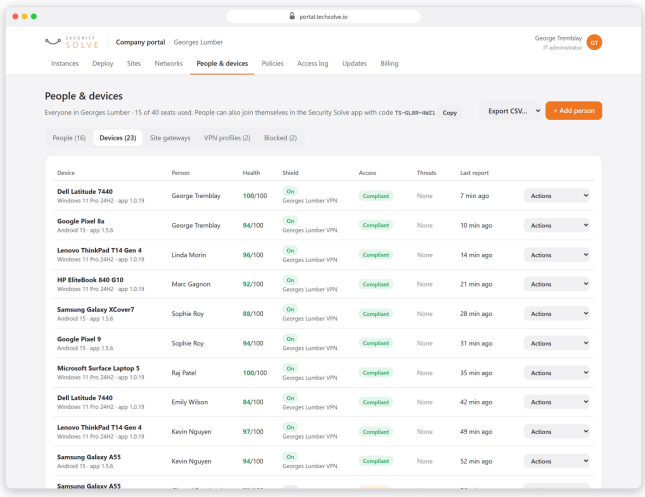


Instances: traffic now, network usage, and a live card for every server, office gateway and machine

- **See everything:** private servers, office gateways and connected machines with status, CPU, traffic, uptime, users and blocked threats; a report as a spreadsheet.
- **Deploy:** request a new server, in the Security Solve cloud, your own cloud account or on your own hardware.
- **Connect offices:** add a site with one install command, or your router.

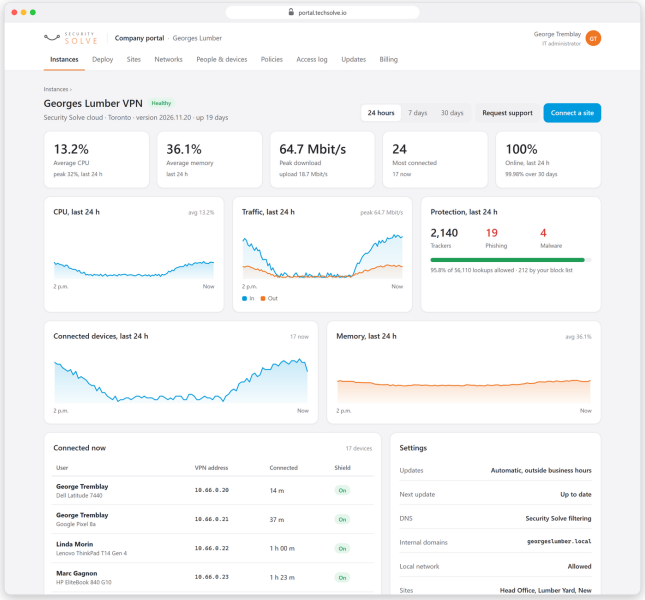


People: staff, portal admins, devices and VPN profiles

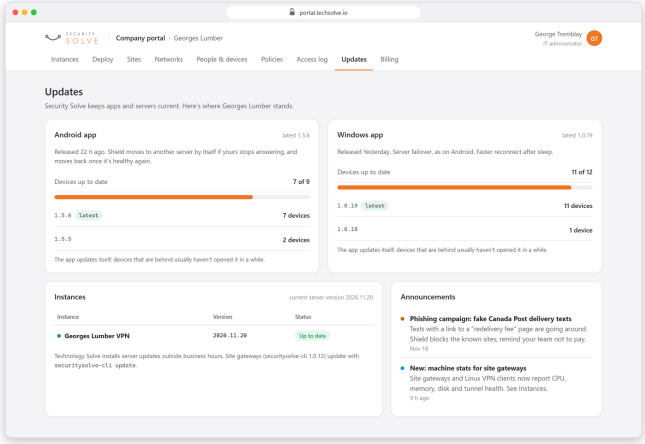


Devices: health, Shield, compliance and threats

- **People and devices:** add staff, reset passwords, create VPN profiles, sign someone out everywhere or suspend them for a set time.
- **Block a lost laptop** or a suspicious address in seconds; it's disconnected within about two minutes.
- **Access log** (optional, your private servers only): see which sites were looked up and what was denied, with your own retention, and export to your cloud storage. Off by default; your people are told in the app.
- **Ask for more:** a new server, support or a plan change, and follow its progress.



Inside a server: CPU, memory, traffic, protection and who's connected

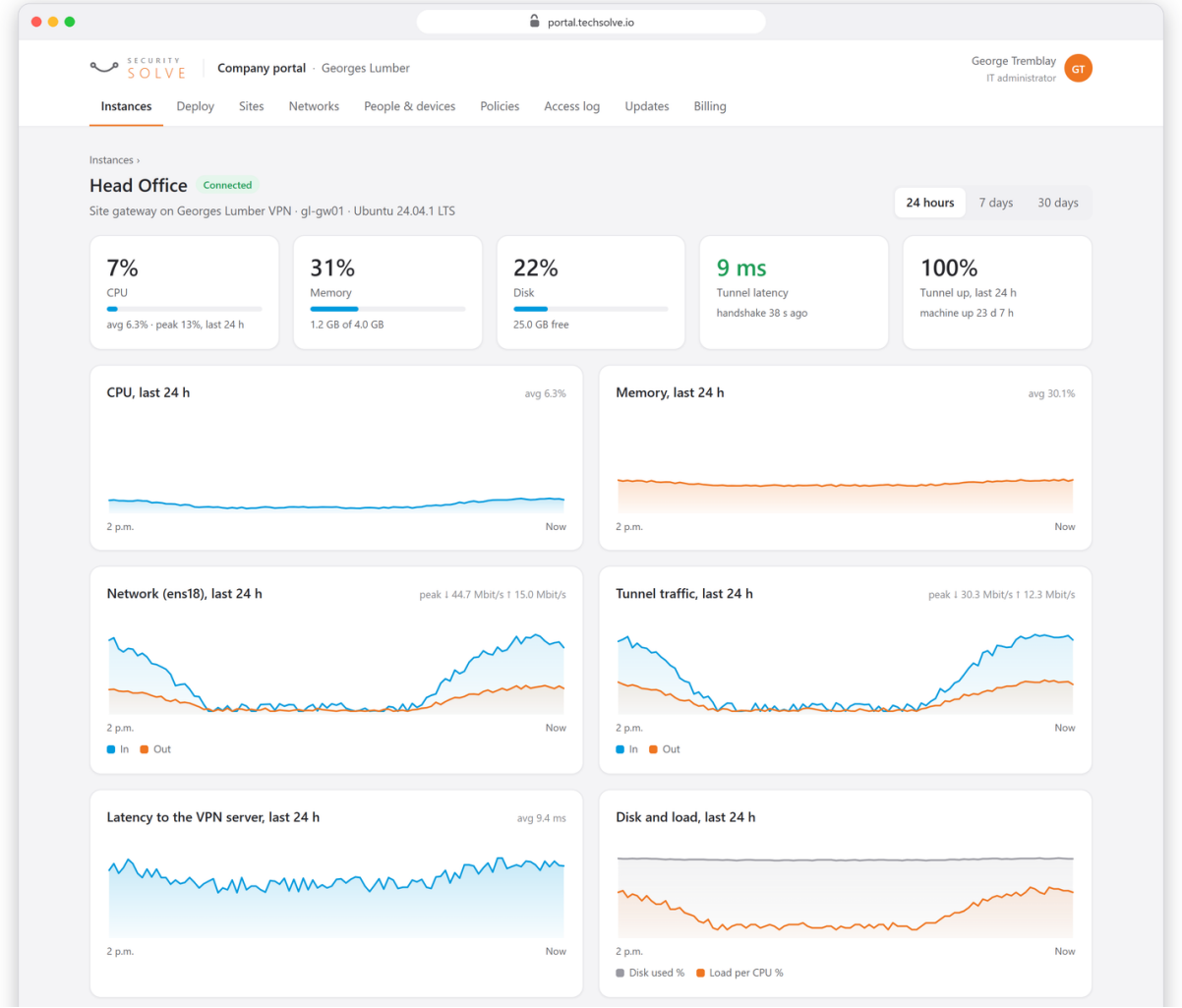


Updates: app and server versions

COMPANY PORTAL

Health for every machine

Your office gateways and Linux machines on the VPN report their health every five minutes, so you see a problem coming before anyone calls about it.



An office gateway: CPU, memory, disk, network, tunnel traffic and latency

- **Graphs over 24 hours, 7 days or 30 days:** CPU, memory, disk, load, office network and VPN tunnel traffic, and latency to your private server.
- **At a glance:** every site in the portal shows its gateway's health, and Office Exit says plainly when it isn't working.
- **Repairs itself:** gateways keep Office Exit and full-tunnel routing working through network restarts, and fix them within minutes if anything changes.

MANAGED SERVICE

Managed for you by Technology Solve

Technology Solve runs Security Solve for you: every organisation, person, device, server and site.

Monitored
Device health and threats for every device, with alerts for anything that needs attention.

Always up to date
Windows PCs update themselves; Android gets a one-tap update prompt. Gateways update daily.

Always available
The control server has a hot standby on separate infrastructure that takes over by itself within minutes, and hands back once the main server is healthy.

Backed up
Encrypted nightly backups, kept 14 days and 12 months.

Messages
Important notices (for example a phishing campaign) reach every device in your organisation.

Microsoft 365
Your staff sign in with their work account and join your organisation automatically.

Secure administration
Two-step verification for administrators; you only ever see your own organisation.

Privacy first
No browsing logs. Activity visibility and access logging are off unless you turn them on, and users are told.

Get started. Talk to Technology Solve: we'll set up your organisation, your private server and your office link, and get your team protected the same day. techsolve.io