SECURITY
SOLVE

Secure by design

How Security Solve protects devices, offices and remote access for small business

Whitepaper · November 2026

by TECHNOLOGY
SOLVE

techsolve.io

EXECUTIVE SUMMARY

Enterprise-grade protection, sized for small business

Small and mid-sized businesses face the same phishing, malware and network threats as large enterprises, usually without a security team. Security Solve gives them one managed platform that protects every device, replaces the exposed remote-access VPN, and filters whole office networks.

1.8M+
phishing and malicious domains blocked, refreshed every 6 hours

0
inbound ports opened at client offices

~2 min
automatic control-plane failover to a hot standby

1 app
for Windows and Android; profiles for Apple devices

Security Solve combines four things that are normally bought, configured and monitored separately:

- **Shield**, an always-on WireGuard VPN that filters every name lookup from every app, so malware, phishing, trackers and unwanted content never load, on any network.
- **Endpoint protection** on the device: malware scanning, a link checker, breach monitoring, Wi-Fi safety checks and a health score reported centrally.
- **Zero-exposure remote access**: a private server per company, and office gateways that connect out, so staff reach remote desktop, file shares and printers with nothing at the office exposed to the internet.
- **Policy and visibility**: per-organisation filtering, device compliance, conditional access and optional access logging, managed by Technology Solve and by the client's own IT in a self-service portal.

This paper explains how the platform is built, how each control works, what data it keeps (and what it doesn't), and how it stays available. It's written for IT decision makers, auditors and technical buyers.

THE PROBLEM

Why small businesses need a different approach

Most attacks on small businesses don't need sophisticated exploits. They need one click, one weak network or one exposed remote-access device.

Risk	What typically happens	Why it's hard today
Phishing	A convincing sign-in page harvests a Microsoft 365 password; the mailbox is used for invoice fraud.	Email filters miss new domains; links arrive by text, chat and social media too.
Malware	A fake update or banking trojan on a phone or PC steals credentials or session cookies.	Antivirus alone doesn't stop the connection to the attacker's servers.
Untrusted networks	Hotel, airport and café Wi-Fi intercept or redirect traffic.	Staff work from everywhere.
Exposed remote access	An internet-facing VPN appliance or forwarded RDP port is scanned and exploited, often within hours of a vulnerability being published.	Appliances need constant patching; port forwards are forgotten.
Tool sprawl	Separate VPN, DNS filter, antivirus and MDM consoles, each half-configured.	No one has time to run them, and nothing ties device health to access.

Design principles

Nothing listens at the office

Sites connect out to their server. There is no inbound port, appliance or forwarded service for an attacker to find.

Filter every app, every network

Filtering happens in the tunnel, at the name lookup, so it covers browsers, apps and background services alike.

Least privilege by default

Each organisation reaches only its own sites, and each site only the machines listed. Sites can't reach staff devices.

Private by default

No browsing logs. Any visibility is opt-in, per organisation, scoped to its own servers, and disclosed to users.

Health decides access

Unhealthy, outdated or infected devices are restricted automatically until they're fixed.

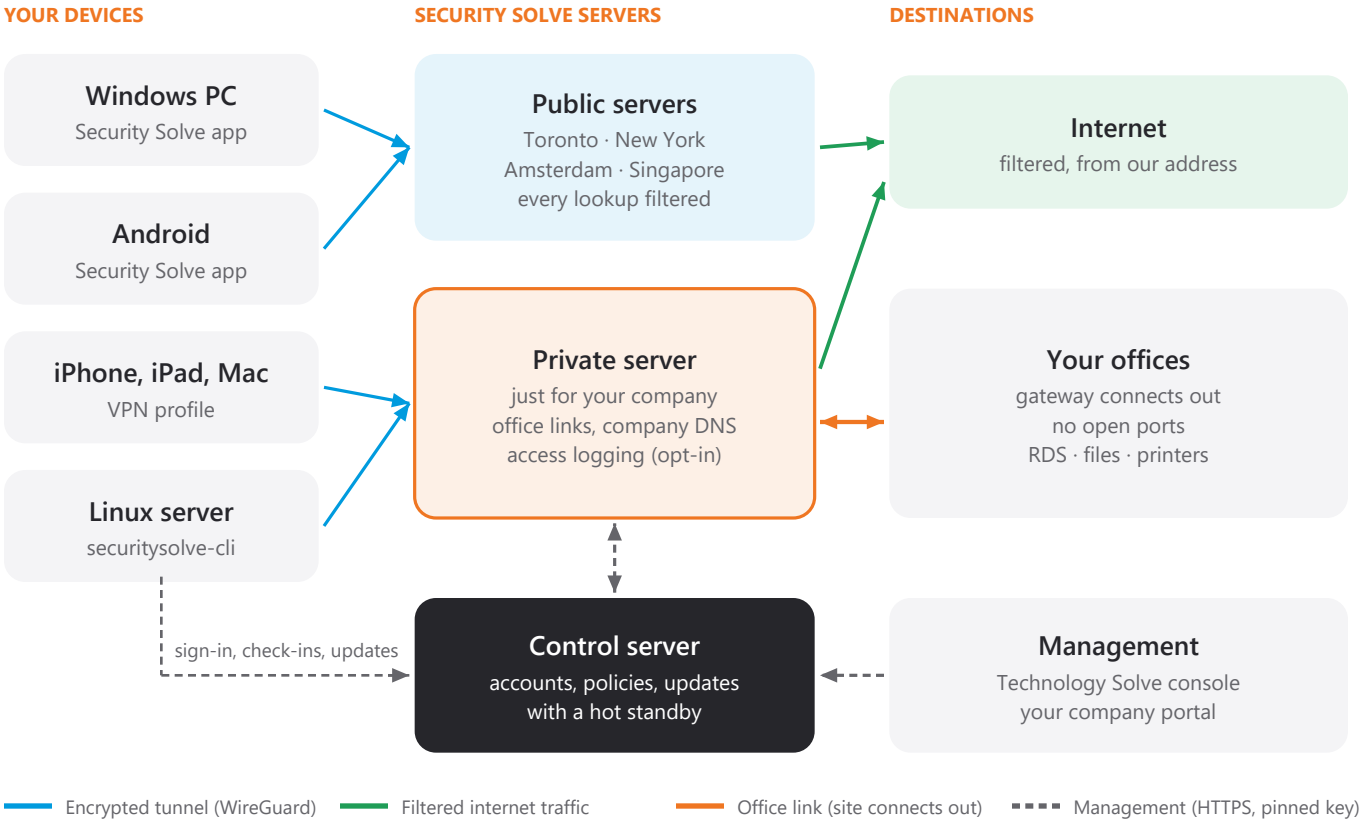
Managed, not just sold

Technology Solve operates, updates and monitors the platform, with the client's IT in control of their own rules.

ARCHITECTURE

Three layers, one platform

Devices connect to Security Solve servers, which filter traffic and link offices. A control server keeps accounts, policies and software in step, and never carries user traffic.



Component	Role	Talks to
Apps and profiles	Windows and Android app (Shield, scanning, health); OpenVPN profiles for iPhone, iPad and Mac; securitysolve-cli for Linux and Windows Server	VPN servers (WireGuard / OpenVPN); control server (HTTPS, pinned key)
VPN servers	Terminate tunnels, filter DNS, enforce firewall rules for sites and policies	Devices, office gateways, the internet; fetch policies from the control server
Office gateways	A Linux VM, Windows Server or router at each site; connects out to its private server	Its private server only (outbound UDP)
Control server	Accounts, organisations, policies, block lists, device reports, updates; replicated to a standby	Apps, servers, portals (HTTPS)
Console and portal	Technology Solve's management console; the client's company portal	Control server, with the signed-in user's session

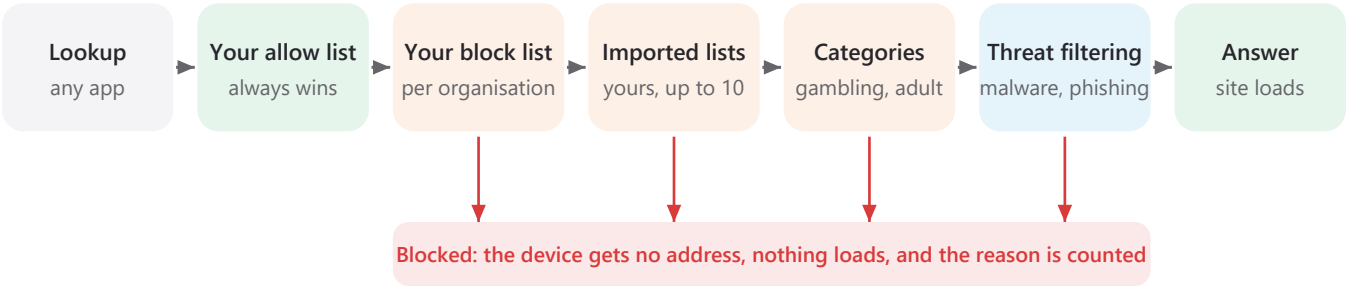
SHIELD

An encrypted tunnel with filtering built in

Shield is a WireGuard VPN. When it's on, all of a device's traffic is encrypted to a Security Solve server, and every name lookup is checked before anything connects.

- **Per-device keys.** Each device generates its own WireGuard key pair; nothing is shared between devices, people or companies. A lost device is cut off by blocking that one device.
- **Filtering at the lookup.** Blocked names get no address, so the page, tracker or malware download never starts. It works for every app, not only browsers, and adds only milliseconds.
- **Bypass resistant.** DNS is locked to the tunnel; Firefox's encrypted-DNS (DoH) canary is blocked so the browser keeps using the protected resolver, and a category blocks known VPN, proxy and Tor bypass services.
- **Local network, safely.** Printers, casting and NAS on the same Wi-Fi are reached directly, while every lookup and all internet traffic stay in the tunnel. Organisations can turn this off.
- **Leaves from our address.** Websites see the server's address, never the user's home or hotel IP.

How a lookup is decided



Layer	What it catches	Controlled by
Allow list	Sites the business needs, even if a list below would block them	The organisation
Block list, imported lists	Specific sites, for a set time or indefinitely; up to 10 of the client's own lists (hosts, Adblock or plain formats)	The organisation
Categories	Adult, gambling, social media, streaming, games, dating, piracy, drugs, crypto, bypass services, AI chatbots	The organisation
Threat filtering	Phishing, malware, ads and trackers from OpenPhish, Phishing.Database and HaGeZi threat intelligence	Security Solve
Access policies	Restrictions for devices that fail compliance (see Conditional access)	The organisation

ENDPOINT PROTECTION

On the device, before and after the click

The network blocks the connection; the app finds what's already there and helps people make safe choices.

Malware scanning

Installed apps are scanned daily and on demand; new installs within seconds. Detects fake system updates, fake banking apps, banking trojans, stalkerware and spyware-like permission sets.

File checks by fingerprint

Before a download is opened, only its SHA-256 hash is sent for checking. The file never leaves the device.

Link Checker

Any link can be checked against the same threat intelligence before it's opened, with the list that flagged it.

Breach monitoring

Work emails are checked against known breaches daily. Password checks use k-anonymity: only the first 5 characters of the password's hash leave the device.

Network safety

Each Wi-Fi network is checked for weak encryption, DNS hijacking and captive portals, with a one-tap prompt to turn Shield on.

Health score

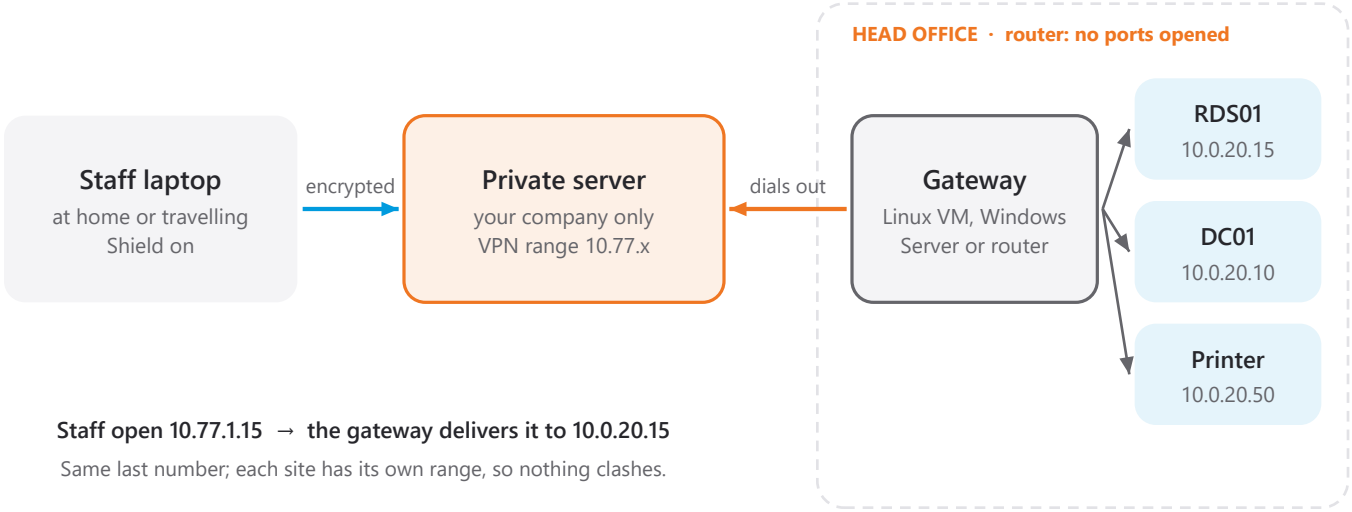
Antivirus, real-time protection, definitions, firewall, disk encryption, Secure Boot, OS version, screen lock and Shield combine into a 0–100 score, reported centrally and used by access policies.

Live connection maps on the device (where each connection went, what was blocked) are kept in memory for one hour and never stored. They exist to help the user, not to monitor them.

REMOTE ACCESS

Zero-exposure access to the office

A private server per company, and a small gateway at each office that connects out to it, replace the internet-facing VPN appliance or forwarded RDP port.



- **Outbound only.** The gateway (a Linux VM, an always-on PC, a Windows Server, or a pfSense, OPNsense or MikroTik router) dials out over UDP. The office router opens no ports and needs no static IP.
- **A range per site.** Each site gets its own VPN range (for example 10.77.1.x for 10.0.20.x), so two offices can use the same LAN range and nothing clashes with staff's home networks.
- **Enforced on the server.** Firewall rules on the private server decide which organisation may reach which site, and, in listed mode, which machines. Office machines cannot open connections to staff devices.
- **Site-to-site links** are one-way and list exact source and target machines, for example one PC at the yard reaching the accounting server at head office.

	Traditional remote-access VPN	Security Solve
Exposure	Appliance or port listening on the internet	Nothing listening at the office
Patching	Client patches the appliance, urgently, often	Managed; gateways update themselves daily
Scope	Often the whole LAN once connected	Per organisation, per site, per machine
Web protection	Usually none, or split tunnel bypasses it	Shield filtering stays on for everything else
Device health	Rarely checked	Conditional access on health, threats and version

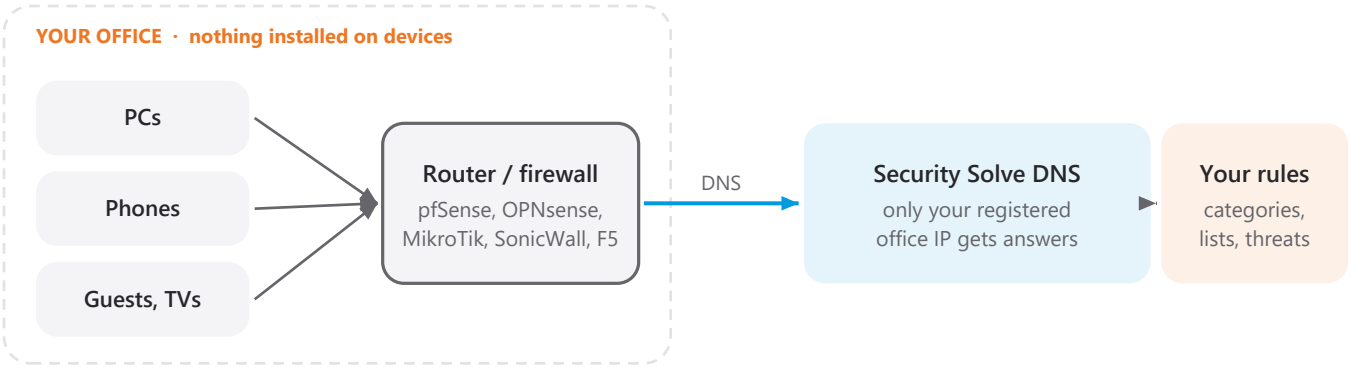
COMPANY DNS

Internal names over the VPN, and whole-office filtering

Private servers relay an organisation's internal domains to its own DNS servers, and router-level filtering extends protection to devices that can't run an app.

- **Internal domains** (for example company.local) are forwarded over the office link to the client's domain controller. Answers are translated into the site's VPN range, and the domain is pushed as a search domain, so rds resolves as it does in the office.
- **Resolver choice** per organisation on its private servers: Security Solve filtering, our unfiltered no-log DNSSEC-validating resolver, or the client's own DNS servers. The organisation's lists apply in every mode.

Network DNS for routers and firewalls



- The client registers each office's public IPv4 address; the router uses Security Solve's network resolvers. Every device behind it, including guests, TVs and IoT, gets the organisation's filtering with nothing installed.
- **Never an open resolver:** only registered addresses get answers, each limited to 300 queries a second; ANY queries are refused and large UDP answers are truncated, so the service can't be used for amplification attacks.
- Dynamic addresses update automatically through a per-network key (DynDNS2-compatible). Guides cover pfSense, OPNsense, MikroTik, SonicWall and F5 BIG-IP, including blocking DNS-over-TLS bypass.

CONDITIONAL ACCESS

Device health decides what's reachable

Access policies connect what the app knows about a device to what the network allows it to do.

Condition	Example
Minimum health score	Below 70: no Microsoft 365
No unresolved threats	Malware found: quarantine until removed
Minimum app version	Older than 1.0.16: block the line-of-business app
Recent check-in	Not reported in 72 hours: restrict

- **Actions**: block chosen domains, or **quarantine** (only listed domains, plus Security Solve itself, still work). Policies apply at the VPN within a minute, to everyone, an organisation, a person or one device.
- **Users are told why** and how to fix it in the app; access returns automatically when the device is healthy again.
- **Instant blocks**: a lost device, or a suspicious address or range, can be blocked for a set time or indefinitely; connected sessions are cut within about two minutes.
- **Identity**: staff sign in with Microsoft 365 and join their organisation automatically. Administrators must use two-step verification (authenticator app, with single-use recovery codes).

PRIVACY

What we keep, and what we don't

Security Solve is built to protect people, not to watch them. Visibility beyond counts is always the organisation's choice, scoped to its own servers, and disclosed to users.

Data	Kept?	Detail
Sites visited (public servers)	No	Filtering servers keep no record of lookups; only counts of what was blocked, by type
Live activity on the device	1 hour, in memory	For the user's own maps; never stored
Activity visible to IT	Off by default	If an organisation turns it on: last hour, in memory; users see a notice in the app
Access log	Off by default	Opt-in per organisation and per private server: time, person, device, site name, allowed or denied, and why. The organisation chooses retention (30 days unless changed) and an optional export to its own cloud storage. Users are notified
Page contents, full URLs, messages	Never	Only site names (DNS) are ever seen
Device reports	Yes	Model, OS and app version, health checks, threats found, server, last report: for support and compliance
Files you scan	Never	Only the file's hash is sent
Passwords you check	Never	Only the first 5 characters of the hash (k-anonymity)

Organisations only ever see their own data. The company portal is scoped to one organisation on the server, not just in the page, and every administrative change is recorded with who made it.

PLATFORM SECURITY

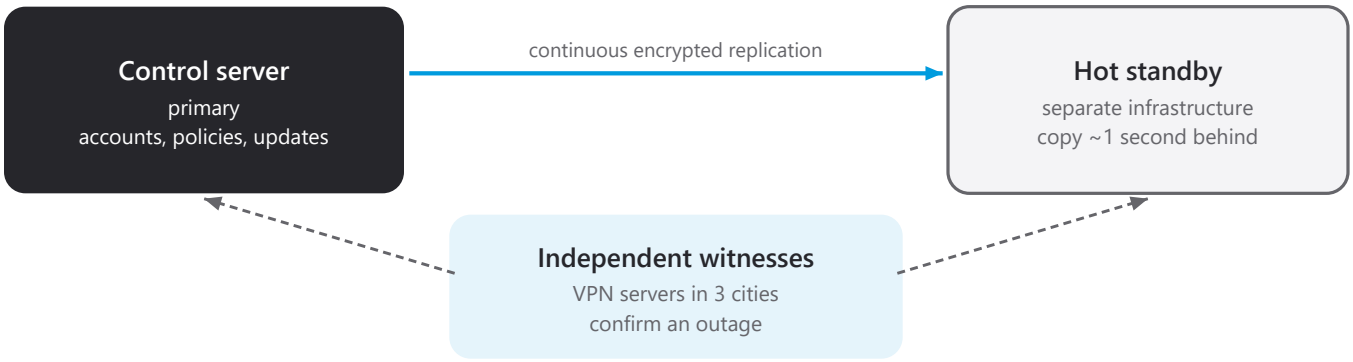
How the platform protects itself

Area	Control
Traffic	WireGuard (Curve25519, ChaCha20-Poly1305) between each device and its server; per-device keys; OpenVPN with per-profile certificates and passwords for Apple devices.
App to control server	HTTPS with the server's key pinned in the apps, CLI and gateways, so a fake or intercepted server is refused.
Office gateways	Enrolment tokens work once and expire after 24 hours; tokens and site keys are stored only as hashes. Gateways connect out and verify the server's key.
Software updates	Windows updates are checked by hash and code signature before installing; an update not signed by Technology Solve is refused. Android updates are signature-checked by the OS.
Web portals	Sessions in HttpOnly cookies, a strict Content Security Policy on the management console, lock-out after repeated wrong passwords or codes, and two-step verification for administrators.
Imported lists	List URLs must resolve to public addresses; the fetch goes to the checked address (no DNS rebinding), redirects are re-checked and downloads are size-limited.
Separation	Each organisation's sites, lists, DNS and logs are isolated server-side; one private server can serve several organisations without them seeing each other.
Auditability	Console and portal changes are recorded with actor and time; organisations see their own activity history.

RESILIENCE

Built to stay up

VPN servers run independently: if the control server is unreachable, tunnels and filtering keep working with the last policies. The control server itself has a hot standby.



- **Continuous replication.** The control server's databases stream to a standby on separate infrastructure, typically about one second behind; configuration and threat feeds follow every minute.
- **Careful failover.** The standby takes over only when it has failed to reach the primary for a minute, at least two of three independent VPN servers in different cities agree it's down, and its own copy is known to be fresh. A network problem on the standby's side can't trigger a takeover.
- **Clients follow by name.** Apps, gateways and servers reach the control server by name and verify its key, so they move to the standby within minutes without reconfiguration. A returning primary can't overwrite newer data.
- **Backups.** Every server is backed up nightly, encrypted on the server before it leaves, to off-site object storage, kept 14 daily and 12 monthly copies, with tested restore tooling.
- **Always current.** Windows apps update themselves within six hours of a release; gateways check daily; servers are updated by Technology Solve outside business hours.

DEPLOYMENT

From agreement to protected, the same day

1. **Organisation.** Technology Solve creates the organisation, connects Microsoft 365 sign-in, and gives the client's IT contact the company portal.
2. **Private server.** Deployed in the Security Solve cloud (Canada by default), the client's own cloud account, or as an appliance on the client's hardware (Proxmox, Hyper-V, VMware). Setup takes minutes.
3. **Offices.** One command on a small VM or server at each site, or a few settings on a supported router.
4. **Rules.** Sites and machines staff may reach, internal DNS, block lists and categories, access policies.
5. **Staff.** Install the app and sign in with their work account; Apple devices get a profile link. Shield is on.

Supported platforms

Platform	How
Windows 10 / 11	Security Solve app; silent automatic updates
Android	Security Solve app (Google Play or direct)
iPhone, iPad, Mac	OpenVPN Connect with a Security Solve profile
Linux servers	securitysolve-cli: Debian, Ubuntu, CentOS Stream, Rocky, Alma, RHEL
Windows Server	securitysolve-cli.exe as a site gateway (split or full tunnel)
Routers and firewalls	pfSense, OPNsense, MikroTik as gateways; any router or firewall for network DNS

Summary

Security Solve closes the gaps small businesses are actually attacked through: the click, the network and the exposed door to the office. It does so with one app, one managed network and one portal, without exposing anything at the office and without logging what people browse unless the business chooses to.

Talk to Technology Solve to see Security Solve on your own network, or to arrange a technical review with your IT team. techsolve.io