Cybird

CYBIRD TECHNOLOGIES / MSP WHITEPAPER

Small Business Network Security
A practical guide for MSPs

How managed service providers can deploy, verify and operate Wi-Fi, threat protection, visibility and resilient connectivity for 5–50 user businesses.

For managed service providers, system integrators and small business leaders

September 2026 | cybird.net

Executive summary

Small business security fails less often for lack of controls than for lack of anyone operating them.

A 25-person firm runs cloud accounting, payments, video calls, laptops, personal phones, printers and visitor Wi-Fi through one router. That router is now the path to daily operations, yet it is usually the least managed device in the building.

MSPs are stuck between two bad options. ISP and consumer routers are cheap but offer little policy, inventory or remote support. Enterprise stacks do everything but need specialists and hours of administration per site. Neither lets an MSP run a profitable, repeatable network security service for 5–50 user clients.

CYBIRD'S PROMISE

A security gateway and cloud console that lets an MSP deploy the same five-control baseline at every small client, verify it with repeatable tests, support it remotely, and show the owner what was done in plain language. Wi-Fi, threat protection, productivity controls and visibility come in one device and one predictable monthly subscription, set up in about 30 minutes. Cybird also scores every device's security posture without an agent, showing the MSP where endpoint, backup and RMM coverage is missing.

This paper sets out that baseline, shows how Cybird maps to it, and gives MSPs a seven-day assessment, acceptance tests and a pilot scorecard they can use with any client.

> **The operating question: Can the MSP prove that the right devices have the right access, that known harmful destinations are blocked, and that the network stays supportable after installation day?**

1 The small business network has changed

One password, one flat network and a few ad hoc exceptions no longer fit how small offices work. Take a clinic with 18 staff: reception, clinicians and visitors share a building but should not share network privileges. A point-of-sale terminal, cameras, printers and personal phones all carry different risks and update cycles. A backup internet line may sit unused because nobody has tested failover.

When something breaks, the old setup gives the MSP nothing to work with. "The internet is slow" could be a WAN fault, a congested access point, a noisy device or a cloud outage. Without device and link visibility, every ticket starts with guesswork, and often with a truck roll.

2 What the evidence says, and what it does not

Ransomware appeared in 88% of breaches at smaller organizations in Verizon's 2025 dataset, against 39% at larger ones. That is the share of analyzed breaches, not any one client's odds of being breached. Verizon's "SMB" group also covers firms up to 1,000 employees, far larger than a typical MSP client.

Ransomware presence among analyzed breaches

Share of breaches involving ransomware; not the probability of a business being breached. Source: Verizon 2025 DBIR SMB Snapshot, pp. 6, 13.

Three other findings from the same report bear directly on the network edge:

22%
of exploited vulnerabilities targeted edge devices and VPNs, up from 3%. Only ~54% were fully remediated, at a median of 32 days.

33%
of SMB breaches involved use of stolen credentials, the leading hacking action. Credential abuse remains the top initial vector.

46%
of infostealer-infected systems holding corporate logins were unmanaged, likely personal BYOD devices.

Source: Verizon 2025 DBIR SMB Snapshot, pp. 6, 8, 13.

No single control covers all of this. Protective DNS helps with known harmful domains but cannot fix a stolen password. Segmentation limits what a compromised device can reach but cannot restore encrypted data. A client plan should state these boundaries up front.

Why the network layer still matters

CISA describes protective DNS as checking queries against threat intelligence before a match is allowed to resolve. Enforced at the gateway, it covers every device on the network, including printers, cameras and phones that cannot run endpoint software. It can be bypassed by encrypted or hard-coded resolvers, and it cannot block domains nobody has flagged yet, so MSPs should test enforcement and treat it as one layer.

3 A five-control baseline

Every small client needs the same five controls, each with a test that proves it works.

This baseline is platform-neutral; Section 5 shows how Cybird delivers it.

Control	What it means	How the MSP proves it
1. Know what is connected	A maintained inventory of every device, its owner or purpose, and its network. Unknown devices are reviewed with the client.	Dashboard inventory reconciled against a physical walk-through.
2. Separate trust zones	At least staff and guest networks; IoT and sensitive systems isolated where warranted, with explicit firewall rules.	A guest device cannot reach business resources; printing still works for staff.
3. Control access by identity	Per-user Wi-Fi credentials instead of a shared password, with a documented join, review and revoke process.	A disabled test account can no longer connect; nobody else is affected.
4. Block known harmful destinations	DNS threat policy for phishing and malware domains, with a clear unblock path and checks on alternate resolvers.	A safe test domain is blocked and logged; a normal business domain resolves.
5. Keep service measurable	Monitoring of WAN links, gateway, Wi-Fi and subscription state; failover tested against real applications.	Primary link pulled in a test window; two critical apps observed and timed.

> **The tests matter more than the settings. A control that has not been tested is a hope, not a control, and a failed test is a work item with an owner, not a checkbox.**

4 Why Cybird

Cybird replaces the pieced-together small office network (router, Wi-Fi, firewall, web filter) with one gateway, one cloud console and one subscription.

Five things make it a fit for MSPs.

1. **It finds the gaps in the rest of the client's security, without an agent.**
   Cybird's device security posture feature scores each device from Poor to Best. It detects AV/EDR, backup and RMM activity from network traffic alone, with no endpoint software, and flags gaps such as missing antivirus, silent backups or unmanaged staff devices. For an MSP, that turns a wall of MAC addresses into a proof-based scorecard, and often into the next service conversation.

2. **All five baseline controls in one box and one plan.**
   Business Wi-Fi, threat protection, content and app controls, and visibility are included in a single predictable monthly subscription, with no per-feature licenses or add-ons. The MSP quotes one line item instead of four.

3 **Fast to deploy, managed from anywhere.**

Cybird is designed to be up and running in about 30 minutes, with no rewiring. After that, policy changes, device checks and troubleshooting happen in the cloud console, not on site. Cybird is built for MSPs, with central management and multi-site support.

4 **Controls that go past the DNS layer.**

Beyond blocking phishing, malware, ransomware and command-and-control domains, the dynamic firewall blocks Tor and direct-IP bypass attempts and detects LAN denial-of-service traffic. App controls block VPN-bypass apps. Upstream DNS is encrypted with DNS over HTTPS. Together these close several of the routes traffic uses to get around a DNS filter.

5 **Reporting owners will actually read.**

A plain-language weekly email covers threats blocked, new devices, busy hours and suggested actions, alongside live dashboards and alerts limited to real issues: outages, risky devices, suspicious activity.

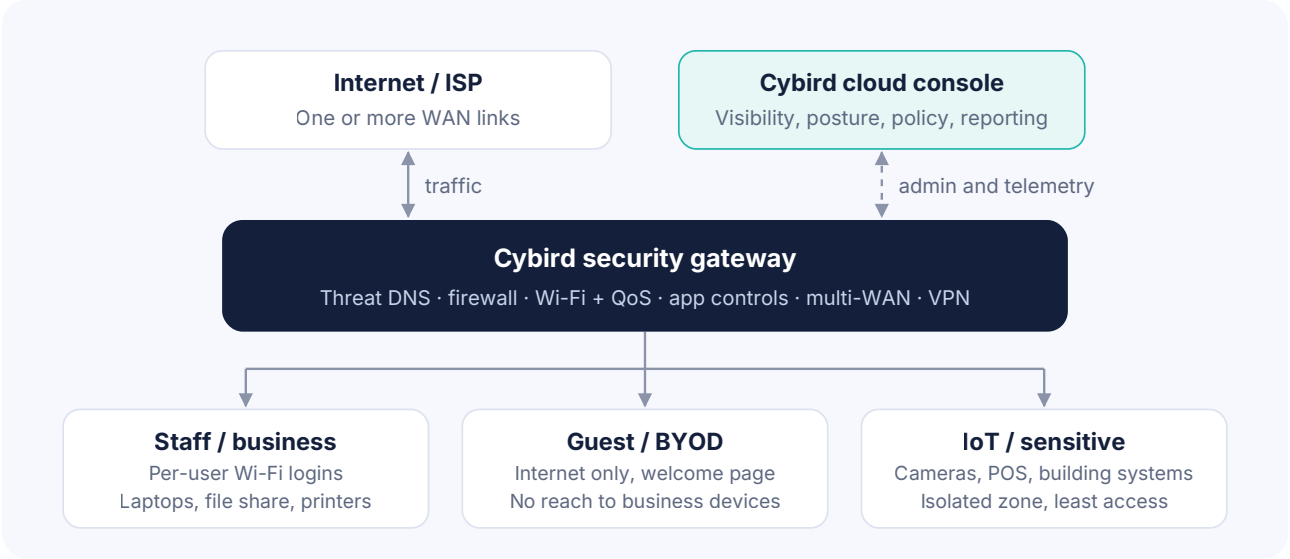
How Cybird compares

Cybird's own positioning against the two alternatives MSPs usually propose:

Outcome	Cybird	Enterprise stack	ISP router
Reliable office-grade Wi-Fi	Included	Included	Limited
Per-user Wi-Fi logins	Included	Usually an extra license	No
Block phishing and malware at the network	Included	Advanced, needs setup	No
Show device risks and missing protections	Included	Separate tool	No
Control distracting apps and sites	Included	Rarely	No
Setup and pricing	About 30 minutes; one monthly plan	Specialist setup; multiple licenses	Minimal setup; limited features

5 How Cybird maps to the baseline

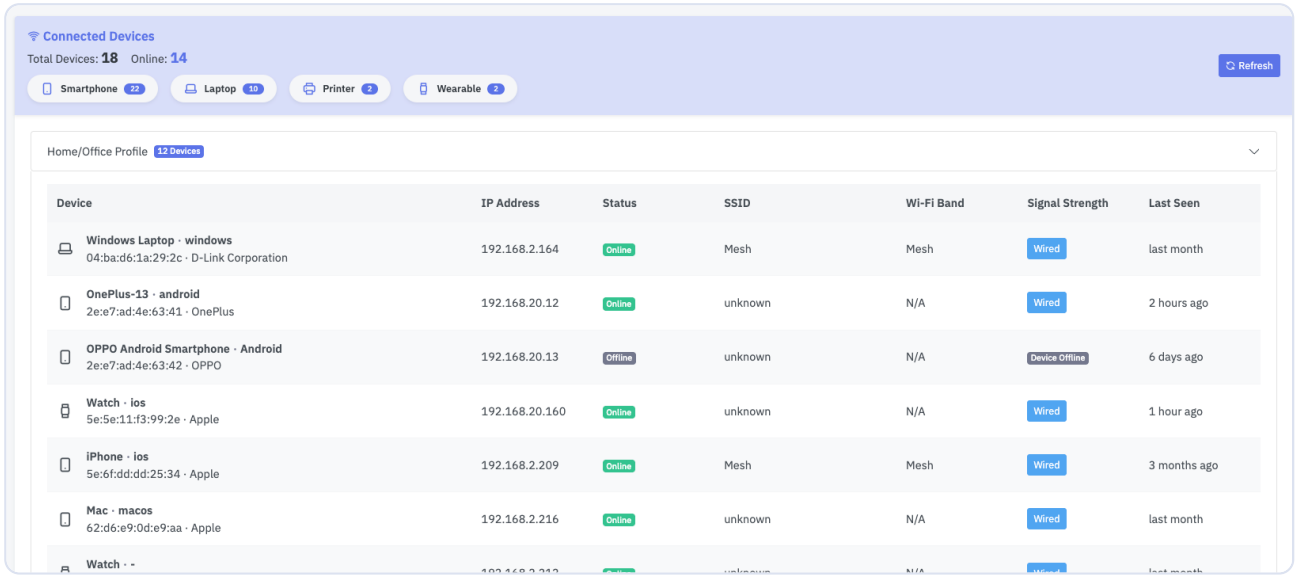
The gateway enforces DNS and firewall policy for every device on every network; the cloud console lets the MSP see status, change policy and investigate events without going on site.



Reference architecture. Customer traffic flows through the gateway only; the cloud console carries administration and telemetry. Endpoint protection, cloud identity and backup stay separate layers in the client's wider plan.

Area	What Cybird provides	How to verify it in a pilot
Business Wi-Fi	Office Wi-Fi with optional mesh coverage and seamless roaming; traffic prioritization (QoS) for Zoom, Teams and VoIP	Walk the office on a call; run a video meeting during a large download
Identity and guests	Per-user Wi-Fi logins for staff; guest network with custom welcome page, password or voucher login, and access-time limits	Revoke a test user; confirm a guest cannot reach office devices
Threat protection	Blocks phishing, malware, ransomware and command-and-control domains at the network, with a block page for users; ad and tracker blocking	Query a safe test domain; confirm the block page and log entry
Firewall	Dynamic firewall that blocks Tor and direct-IP bypass attempts and detects LAN denial-of-service traffic; IoT devices kept in an isolated zone	Attempt a bypass from a test device; confirm IoT cannot reach staff devices
Privacy	Upstream DNS encrypted with DNS over HTTPS	Confirm the resolver setting in the console
Productivity controls	Web category and app blocking (social media, games, streaming, VPN-bypass apps); policies by role (front desk, managers, finance) and by network (staff, guest, IoT)	Apply a role policy to a test user; confirm it takes effect

Area	What Cybird provides	How to verify it in a pilot
Visibility	Live device list; bandwidth by user, device and application; network health dashboard; real-time alerts; weekly email summary	Reconcile the device list against a walk-through
Device security posture	Agentless per-device score (Poor to Best) from detected AV/EDR, backup and RMM traffic, with gaps flagged	Compare scores against the MSP's own RMM and backup records
Resilience	Multi-WAN with automatic failover	Pull the primary link in an agreed window; time the switchover
Multi-site and remote	Secure Office Link (site-to-site VPN for shared printers, NAS, CCTV and apps); Remote Access (employee VPN governed by identity and Cybird policy)	Reach a head-office printer from the branch and from a remote laptop
Management	Cloud console with central management and multi-site support	Confirm admin roles, remote access, alert routing and reporting



Cybird console: connected-device list with device type, IP address, status, network and last-seen time.

What needs design work

Segmentation, role policies, failover and multi-site setups are configured per client and should be validated with the tests in Section 7. Secure Office Link and Remote Access are newer features; scope them after a demonstration on the client's release. Cybird's Office Presence feature, which logs when staff devices join office Wi-Fi, is employee monitoring: enable it only with written staff notice and a check against local employment and privacy law.

6 Running it as a managed service

A platform becomes a service only when the MSP defines who does what, when, and what the client sees.

The service agreement should name who approves blocks and unblocks, who responds to WAN events, how urgent access changes are handled, and what is reviewed each month.

Stage	Partner activity	Evidence delivered
Assess	Inventory devices and links; identify sensitive workflows	Site diagram, access matrix, risk and dependency list
Deploy	Configure staff and guest access, DNS policy, WAN monitoring, admin roles	Configuration record and passed control tests
Operate	Triage alerts, maintain inventory, handle changes and renewal	Ticket trail and a one-page monthly report
Improve	Review exceptions, incidents, new devices and growth	Prioritized change plan with owner and date

A seven-day assessment

Days 1–2 Interview the owner and IT contact. Map internet circuits, switches, access points, users and critical applications.

Days 3–4 Build the device inventory. Flag shared credentials, guest exposure and unmanaged equipment.

Day 5 Draft the target segmentation and DNS policy, starting from a traffic matrix: who needs what, and what should be denied.

Day 6 Agree the failover test, change window and support escalation path.

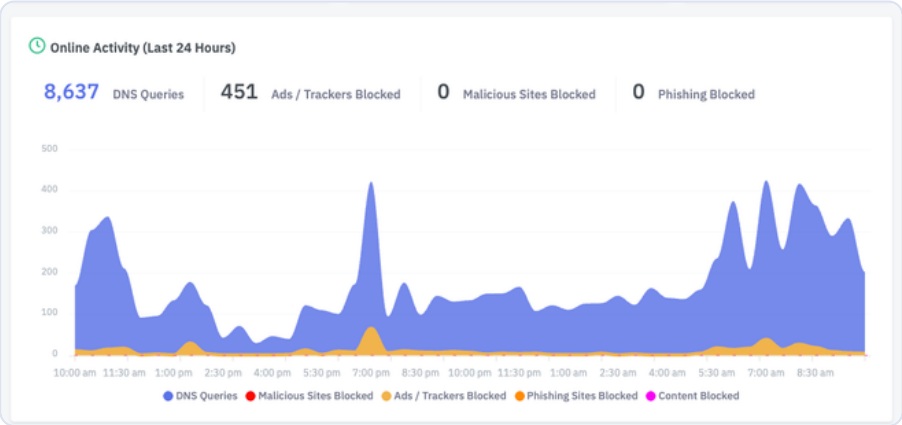
Day 7 Present a one-page baseline, exceptions, expected effort and review plan.

The assessment should also list controls outside the gateway: multifactor authentication, endpoint updates, tested backups and supplier access. NIST's CSF 2.0 Small Business Quick-Start Guide organizes security across Govern, Identify, Protect, Detect, Respond and Recover; network work contributes to several functions but not the whole program.

The monthly report

Cybird's weekly email summary covers the week-to-week view; the monthly report is the MSP's own, one page an owner will actually read: known and new devices, meaningful threat events, outages and failover tests, significant changes, open exceptions, subscription state and the device posture scorecard, with one sentence on any item that needs a decision.

Report confirmed incidents separately from raw DNS block counts, which can be large without meaning much. Every line should trace to a ticket, device, policy change or test result, and log retention should be agreed before the service starts, especially where employee activity is visible.



Cybird console: 24-hour activity showing DNS queries alongside malicious, phishing, ad/tracker and content blocks.

7 Example: a 25-person accounting firm

This is a planning scenario, not a measured deployment. The firm has one office, 25 staff, hard tax-season deadlines, one shared Wi-Fi password, and a mix of company laptops, personal phones and printers. A second internet line has never been tested. The MSP drives on site for basic questions because the old router gives it no remote view.

Before	Proposed setup with Cybird	What changes for the MSP and owner
One shared Wi-Fi password	Per-user staff logins; guest network with a welcome page	Offboard one person without resetting everyone
No reliable device list	Live device list, labeled and reviewed	Spot an unfamiliar device; route tickets to the right owner
Unknown endpoint coverage	Device security posture scorecard	See which laptops lack EDR or recent backups before an incident
No harmful-domain policy	DNS threat protection plus bypass blocking, tested	Known malicious destinations blocked on managed paths
Client video calls freeze at busy times	QoS priority for Teams, Zoom and VoIP	Calls stay clear during large uploads at tax deadlines
Primary link outage stops work	Dual-WAN failover, tested	Critical cloud apps have a documented recovery path
Ad hoc support and renewal	Weekly Cybird summary plus a monthly MSP review	Service state and open actions visible to the owner

Acceptance tests

Run these at go-live and after any material change. Record the date, firmware version, test device, observed result and any exception.

- [ ] Connect one device to each network; confirm its intended internet and local access.
- [ ] Confirm a guest device cannot reach the file share, and an IoT device cannot reach staff laptops.

- [ ] Disable a test employee account; confirm reconnection fails.
- [ ] Query an approved security test domain; confirm the block page and log entry, and that a normal business domain still resolves.
- [ ] From a test device, try an alternate DNS resolver and a VPN-bypass app; confirm both are blocked.
- [ ] Check the posture scorecard against the MSP's RMM and backup records for three devices.
- [ ] Disconnect the primary WAN; time the switchover and note how two critical apps behave. Restore it and confirm traffic returns as intended.

A failed test becomes a work item with an owner. It is never a reason to mark a control complete.

8 Pilot scorecard and quarterly review

Use one representative office and mark each line pass, exception or follow-up. The pilot is done when client and partner agree on the results, the remaining work and who owns each open item.

Question to test	Evidence to keep	Result
Can a new user join and a departing user be removed cleanly?	Account change record; failed reconnection after revocation	
Can guests reach only what is intended for them?	Traffic test from guest Wi-Fi to internet and local resources	
Are the expected devices visible and identifiable?	Dashboard inventory reconciled against a walk-through	
Does the posture scorecard match reality?	Scores for three devices compared with RMM and backup records	
Does DNS policy block a safe test target without disrupting work?	Test result, policy state, exception procedure, log entry	
Are common bypass routes closed?	Alternate resolver and VPN-bypass app tests	
Does failover behave acceptably for the client?	Observed link transition and critical-app behavior	
Can the MSP support and report on the site remotely?	Role permissions, alert routing, a sample ticket and monthly report	

Score nothing from a screen shown in isolation. Pair every demo with a real device, a real policy decision and a recorded result.

Questions the client should ask each quarter

- ? Can we name every active device and its owner or purpose?
- ? Are guests, staff and sensitive systems separated, and when was that last tested?
- ? Which malicious-domain requests were blocked, and which false positives were reviewed?
- ? Can we remove one employee's Wi-Fi access without changing a shared password?
- ? What happened during outages and the last failover test?
- ? Are firmware, threat feeds, subscriptions and support ownership current?
- ? Which policy exceptions exist, who approved them, and when are they reviewed?
- ? What security responsibilities sit with endpoint, identity, SaaS and backup providers?

> **For a small business, security that is consistently deployed, tested and maintained beats advanced controls that nobody operates.**

Start a pilot

Pick one client site and run the scorecard above with Cybird. Setup takes about 30 minutes; the seven-day assessment and acceptance tests follow. At the end, you and your client will have a tested baseline, evidence for every control, a posture scorecard for every device, and a clear decision on rollout.

partners@cybird.net

cybird.net

Sources

1. Verizon, 2025 Data Breach Investigations Report: Small- and Medium-Sized Business Snapshot, pp. 6, 8, 12, 13. verizon.com/business/resources/infographics/2025-dbir-smb-snapshot.pdf
2. CISA, Protective Domain Name System (DNS) Resolver. cisa.gov/resources-tools/services/protective-domain-name-system-dns-resolver
3. NIST, Cybersecurity Framework 2.0: Small Business Quick-Start Guide, SP 1300, February 2024. doi.org/10.6028/NIST.SP.1300
4. Cybird, Features: Small Businesses, V2, September 2026.

Product descriptions reflect Cybird materials as of September 2026 and depend on plan, hardware, software and configuration.