SMSYS SHIELD · WHITE PAPER · JUNE 2026

One outcome, one bill.

A different way to run IT and security for a small business. One team. A score that tells the truth. Proof you can read every month.

The stack nobody designed

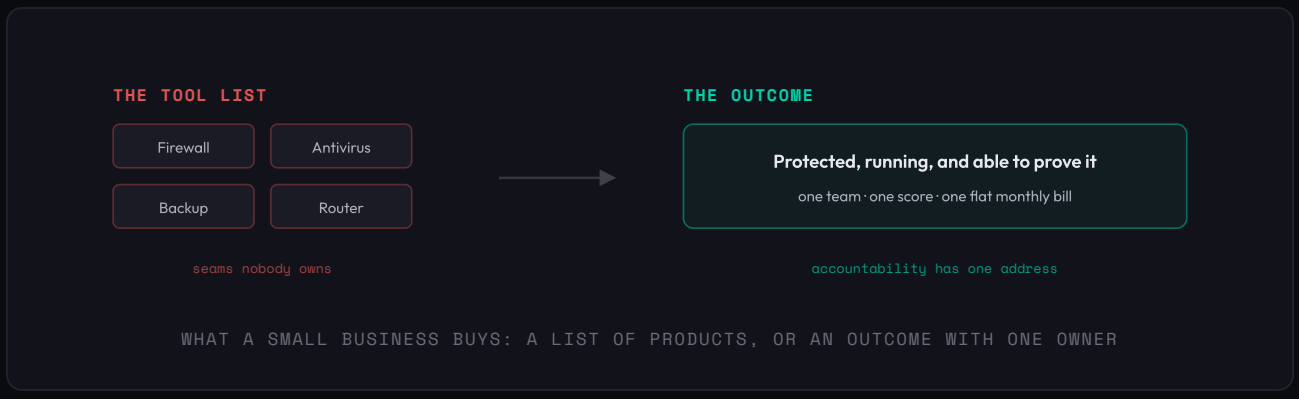
A fifteen person office runs on more technology than a midsize company did a decade ago. Email, files, phones, WiFi, cameras, laptops, a dozen logins per employee. Each piece arrived one decision at a time: a router from a big box store, an antivirus subscription that renews itself, a backup tool someone set up in 2021. Nobody designed the stack. It accumulated.

The accumulation has a price. Attackers automate their way into small offices through the gaps between tools. Insurance carriers ask hard questions before they quote, and they want evidence, not product names. Protection that works stays invisible, so when the invoice arrives, it reads like a question mark. And the owner becomes the integration point: the one person expected to notice when something quietly stops working.

Shield is our answer. Managed IT and security sold as **one outcome on one flat monthly bill**: the business is protected, running, and able to prove both. One team runs the network, locks down the data, sets up the people, and picks up the phone. The work is graded by a security score that measures what actually protects the business, whoever sold the control. The grade arrives every month in a report written in plain language: what happened, what changed, what it was worth.

This changes what a small business buys. Not a list of tools to operate. Not a stack of vendor relationships to referee. A number that goes up and stays up, with receipts.

That is the product.



WHAT A SMALL BUSINESS BUYS: A LIST OF PRODUCTS, OR AN OUTCOME WITH ONE OWNER

Seams nobody owns

The typical small business buys technology the way a house accumulates furniture. A firewall from one vendor. Antivirus from another. A backup subscription, a password spreadsheet, a wireless router in a closet. Each purchase solved the problem of its moment. Together they form a stack nobody designed, with seams nobody owns.

The seams are what attackers use. Breaking in stopped being a craft and became a scan: automated probes that hunt for the old account still active after a departure, the laptop two months behind on updates, the login with no second step. No single tool covers another tool's gaps, and no vendor on the list is responsible for the whole.

88%	$427	$8,300
of small business breaches involve ransomware, more than double the rate at large companies.	per minute: the average cost of downtime for a small or midsize business.	median annual cost of cyber incidents for a small business. A bad year looks nothing like the median.
VERIZON DBIR, 2025	DATTO	HISCOX

Then the insurance renewal arrives. Carriers now ask about multi-factor login, protection on every device, and tested backups before they quote, and they ask for evidence. The questionnaire does not care which products are installed. It cares whether the controls hold.

Through all of it, the deepest flaw hides in plain sight: **protection that works is invisible.** A blocked intrusion looks exactly like a quiet Tuesday. Months pass, nothing visibly happens, and the monthly invoice raises a fair question: what did the money buy? The tool-list model has no answer. It can show receipts for products. It cannot show evidence of protection.

Those are different things.

One outcome, one bill

Shield inverts the model. The business buys one outcome: protected, running, and able to prove it. One team is accountable for the whole stack. One flat monthly bill covers it, with no contracts. Four layers make up the service.

01

The score

A security score from 0 to 100 grades the controls that matter: who can log in and how, whether devices stay current, whether the company's email can be spoofed, whether backups actually restore. The score is the spine of the service. Every gap it finds becomes a work item. Every work item closed moves the number.

02

The protection

Identity with multi-factor login enforced. Protection on every device. Email security and domain protection. Business-grade network gear, segmented and watched. Backups kept offsite, locked against tampering, and test-restored on a schedule the report names. The platforms underneath are established and deliberately boring. Clients buy the outcome, never the brand names.

03

The operations

A helpdesk where a person picks up. A new hire starts Monday with email, logins, and a ready laptop the same day. A departure shuts off every account at once. Updates, slowdowns, and warning signs get handled in the background, most before anyone has to report them. Software watches around the clock. People make the judgment calls.

04

The front office

Two working services no commodity IT provider includes: call handling that answers every call on the first ring, day or night, books appointments, and texts confirmations; and payment follow-up that works overdue invoices courteously and persistently. We built both, so we can include both.

The four layers sell as one thing because they fail as separate things. A patched laptop on a flat, unwatched network is one stolen password from disaster. A perfect backup that has never been test-restored is a hope, not a plan. The score sits underneath all of it, grading the whole, so a gap in any layer shows up in the same number.

One number to watch. One team to call. One bill to pay.

04 · THE SCORE

A score that doesn't sell you anything

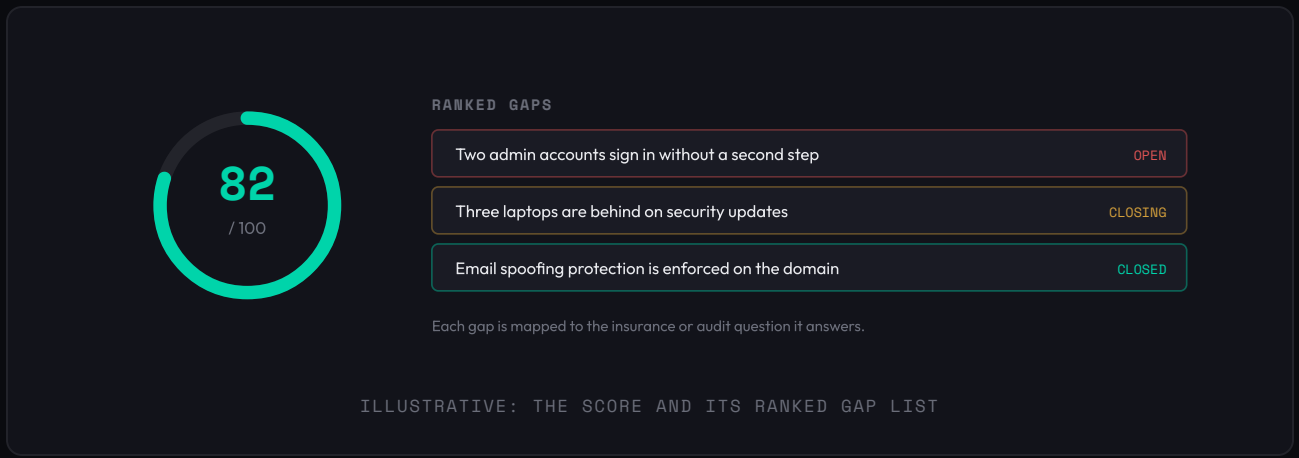
Every major platform offers to score a business's security. The catch sits in the scoring rules: the grader is also the seller. The most widely used measure, Microsoft Secure Score, rises as a business adopts more Microsoft products. It is a useful signal and a conflicted messenger. An office running excellent controls from other vendors can score worse than one that simply bought more from the grader.

> Vendor scores measure how much of the vendor you bought. The Shield score measures what protects you.

The Shield score has one allegiance: does the control hold? Multi-factor login counts the same whichever vendor enforces it. A tested backup counts, whoever sold the software. An exposed service costs points, whatever logo is on the box. The yardstick is not for sale, which is the only reason it can be trusted to measure progress.

The first read costs nothing and takes minutes. Connect Microsoft 365 and the score reads live settings once, keeping no access afterward. Businesses on other platforms take an eight question check. Either way the result is a number, and under the number a ranked list of gaps in plain language, each mapped to what an insurance carrier or auditor would ask about it. The score also grades what is visible from the public internet: whether the company's email can be impersonated, whether its web traffic is encrypted, what services are exposed.

Then the score does its real job. The free assessment becomes the 30-day plan. The 30-day plan becomes a climbing number. The number becomes the monthly report. Progress stays visible because the yardstick never changes.



ILLUSTRATIVE: THE SCORE AND ITS RANKED GAP LIST

05 · THE MONTHLY REPORT

Protection you can read

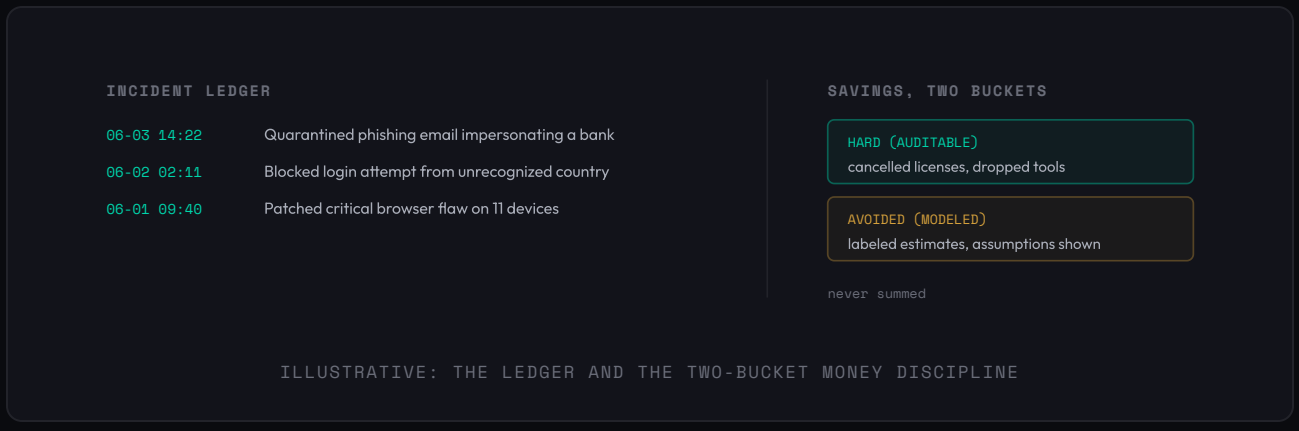
Most of what a security service does right is silent. The Shield monthly report exists to break that silence. It is written for an owner, not an administrator, and it answers three questions: what happened, what changed, and what it was worth.

What happened. An incident ledger in plain language, each line timestamped. Quarantined a phishing email impersonating a bank. Blocked a login attempt from an unrecognized country. Patched a critical browser flaw on eleven devices. Protection stops being a feeling and becomes a record.

What changed. Every known gap, listed as open, closing, or closed, next to the same score as last month. The work either moved the number or it didn't, and the report says which.

What it was worth. Money, reported with discipline. The report splits savings into two buckets and never adds them together. Hard savings are auditable cash: cancelled licenses, dropped duplicate tools, right-sized plans. Roughly half of paid software licenses go unused (Zylo measures 53%), so the audit usually finds something. Avoided costs are estimates: downtime that didn't happen, breach exposure that went down. Every such line carries its assumptions and the word "modeled." A single blended savings number would read better. It would also deserve no trust. The separation is the point.

The report also keeps a standing insurance readiness checklist, mapped to the questions carriers actually ask: multi-factor login on email, remote access, and admin accounts; protection on every device; backups tested, with the date of the last test. Carriers lead with multi-factor login because the evidence is lopsided: Microsoft measures that it blocks 99.9% of automated attacks on accounts. When the renewal questionnaire arrives, the answers are already written down.



ILLUSTRATIVE: THE LEDGER AND THE TWO-BUCKET MONEY DISCIPLINE

Routine work for software, judgment for people

The fixed-before-you-notice model runs on a strict division of labor. Software watches everything, all the time: logins, devices, mail flow, backups, network traffic. It handles the routine volume, the password reset, the false alarm, the patch that should go out at 2am. People handle everything that calls for judgment.

The division has hard edges, and they are written down. Routine, reversible actions happen automatically. Consequential actions are proposed by the system and approved by a person before anything moves. High-impact actions, the kind that touch every account or wipe a device, are carried out by people, full stop. The line never moves on its own.

And someone stays reachable. Printer down, email bouncing, login locked: call, text, or email, and a person picks it up and owns it to the end. Automation makes the service fast. The reachable human makes it dependable.

The same engineering shows up at the front desk. A new customer calls at 9pm on a Tuesday and no one is at the office. The call gets answered on the first ring anyway. The appointment lands on the calendar, the confirmation goes out by text, and the morning starts with bookings instead of callbacks. Overdue invoices get the follow-up calls that never quite fit into anyone's afternoon: courteous, persistent, and on time.

These two services, call handling and payment follow-up, come with Shield because we built them ourselves. They run on the same watched infrastructure as everything else, and no commodity provider can bundle them. They quietly change the math of the engagement: the IT line item starts answering the phone and recovering revenue.

Most IT bills only cost money.

07 · GETTING STARTED

Start with the number

The first step costs nothing and takes minutes. Connect Microsoft 365 for a live read of where the business stands, or answer eight questions for an estimate. Either way the result is a score, a ranked list of gaps in plain language, and a free 30-minute call to walk through both. We read the score once and keep no access.

For businesses that move forward, the findings become a 30-day plan, the plan becomes a climbing score, and the score becomes a monthly report with a ledger, a gap list, and honest math. Flat monthly bill. No contracts. The work speaks every month, in writing, and the number on the first page either went up or it didn't.

What's your security score?

snsys.ai/solutions/shield · (203) 800-6148

SOURCES

- Verizon, 2025 Data Breach Investigations Report: 88% of small business breaches involve ransomware.
- Datto: average downtime cost of $427 per minute for small and midsize businesses.
- Hiscox, Cyber Readiness Report: median annual cyber incident cost of roughly $8,300 for small businesses.
- Microsoft: multi-factor authentication blocks 99.9% of automated attacks on accounts.
- Zylo: 53% of paid SaaS licenses go unused.

About SNSYS. SNSYS (pronounced "Senses") builds and runs technology for small businesses: managed IT and security, call handling, payment follow-up, cameras, WiFi, and websites, delivered as one connected system with one team behind it. Shield is the managed IT and security service. Learn more at snsys.ai.