



TRUSTIVUM

Secure first. Audit-ready as the result.

A quick overview of **Trustivum:Compliance**, the guided compliance platform for small regulated businesses, and the three add-on services that make the daily security work happen and turn it into evidence.

THE PLATFORM

Trustivum:Compliance

Governance, risk & compliance

ADD-ON

Trustivum:ComplianceDesk

Service desk & evidence collection

ADD-ON

Trustivum:ComplianceLedger

Asset management

ADD-ON

Trustivum:ComplianceVector

Penetration testing & security validation



The point is not to pass an audit. The point is to be secure.

An audit only checks whether the security work happened. Trustivum makes it happen: access comes off on time, the asset list stays true, the network gets tested, policies get followed. When the work happens inside the tools, the evidence writes itself. Passing the audit becomes the byproduct of running a secure business.

DO THE WORK

Trustivum: ComplianceDesk

Access, incidents, vulnerability fixes, changes and periodic reviews run as tracked workflows with the right approvals and deadlines.

KNOW WHAT YOU HAVE

Trustivum: ComplianceLedger

Every device, system, app and data store with an owner, a protection posture and a data-flow map.

PROVE IT HOLDS

Trustivum: ComplianceVector

Penetration testing and scheduled security validation, outside and inside the network, with retests tracked to closure.



Trustivum: Compliance

The program of record. Controls, policies, weekly prompts, coaching and the evidence vault.

- Process evidence from the Desk
- Inventory and data-flow evidence from the Ledger
- Testing evidence from Vector
- Everything else from the weekly prompts

The readiness view shows what is done, due and missing.



Secure, and able to prove it

The auditor reviews through the portal. Customers, partners and insurers get straight answers.

- SOC 2 Type 1, then Type 2
- HIPAA compliance posture on record
- Security questionnaires answered from evidence, not memory
- Next year's improvements already scheduled

Standalone by design

None of the add-ons requires the platform, and the platform works without them. Connections add automation, never dependency.

Start anywhere

Begin with whichever one your auditor, customer or insurer circled. Each add-on is its own subscription; grow into the rest when the work demands it.

Built for small teams

Healthcare practices, their vendors, B2B SaaS and any growing company with 20 to 200 people and no compliance staff.



Trustivum: Compliance

A guided compliance platform for the company run by the IT admin who already has five other jobs. It tells you what to do, asks the right people the right questions, keeps the proof, and gives the auditor a front door.

Pick a framework, get a program

Choose SOC 2 or HIPAA, or both. Trustivum maps the controls, hands you policies written to be adopted rather than edited for a week, and lays out the year.

Weekly prompts, not just a dashboard

Three to five short questions a week go to the people who do the work, over Slack, Teams or email. Their answers and attachments land as evidence on the right control.

Trusty, the compliance coach

An assistant that knows your company and explains every control in plain English. It nudges when something slips and gets quieter as the team gets better.

Evidence vault and readiness view

One place for every policy, answer, document and test result, with a clear view of what is done, what is due and what is missing before the audit.

Auditor portal

The auditor reviews controls and evidence from the same system, scoped to their engagement. No binder, no shared drive, no month of email.

Built for the second audit, too

After a Type 1 report, the auditor's list of improvements becomes next year's prompt schedule. You walk into Type 2 already prepared.

Pricing

\$600 / month

+ \$950 one-time setup · one framework (SOC 2 or HIPAA)

- Second framework adds \$350 a month; third and each additional adds \$300
- Setup is charged once per customer, not per framework
- Annual billing available at a discount; 30-day money-back
- **Covers the compliance application only.** ComplianceDesk, ComplianceLedger and ComplianceVector are separate add-ons that increase your monthly.

Who it is for

- ✓ B2B SaaS, healthtech and healthcare IT companies with 20 to 200 people
- ✓ Teams being asked for SOC 2 or HIPAA readiness by a customer, partner or insurer
- ✓ Medical and dental practices and the vendors who serve them
- ✓ The technical operator told to "get us ready" with no compliance staff



Trustivum:ComplianceDesk

A compliance-native work desk. Every security task a regulated small business has to do runs as a tracked workflow, and every finished workflow is a piece of audit evidence.

A general helpdesk proves a ticket was closed. An auditor, a regulator or a cyber insurer asks harder questions: who requested it, who approved it, who did it, were they different people, did each step happen inside the required time, which control does it satisfy, and can you prove the record was not changed afterwards?

ComplianceDesk is built around those questions. Granting and removing access, handling an incident, fixing a vulnerability, approving a change, testing a backup, reviewing a vendor, reviewing who has access: each runs as a defined workflow with enforced steps, named approvers and deadlines. When the ticket closes it produces a tamper-evident evidence package mapped to SOC 2, HIPAA and ISO 27001 controls.

Eleven workflows, day one

Access request and removal, incident, vulnerability fix, change, backup test, DR drill, vendor review, policy exception, access review, asset check.

Tamper-evident record

Every action lands in an append-only, hash-chained log anyone can verify. The evidence package carries its own proof.

Auditor-ready by default

An auditor reviews evidence through a time-limited, read-only link. Nothing to export, nothing to reconstruct.

Where it fits

- Works fully standalone for any small regulated business
- Pushes evidence into Trustivum:Compliance automatically
- Receives findings from Trustivum:ComplianceVector as remediation tickets
- Knows the asset behind every ticket from Trustivum:ComplianceLedger

Pricing

Add-on

pricing on request · separate from the Trustivum:Compliance subscription

Includes all eleven workflows, the compliance calendar, evidence packages, auditor links and export. Two-factor sign-in required for everyone who works or approves tickets.



Trustivum:ComplianceLedger

The asset inventory an auditor can actually trust. Every device, system, application, cloud resource and data store: who owns it, what data it holds, how that data moves, whether it is protected, and what happened to it from purchase to disposal.

Every framework starts with an inventory. SOC 2, HIPAA, ISO 27001, the CIS Controls and the NIST frameworks all assume you know what you have before you can protect it. Most small businesses keep that list in a spreadsheet with no owner, no record of where patient or customer data moves, no proof a laptop was wiped before it left, and no way to notice a device that appeared on the network but never made the list.

ComplianceLedger replaces the spreadsheet with a living register. Each asset carries an owner, a data classification, a criticality and a protection posture: encryption, multi-factor login, endpoint protection, patching and backup, each with a source and a freshness date. Disposal cannot be recorded without a sanitization record. Discovery imports go through a human-confirmed reconciliation queue, so nothing merges silently.

Data-flow map

See where sensitive data lives and how it moves between systems, exportable for the auditor and for a HIPAA risk analysis.

Certified snapshots

Periodic reviews produce a hashed inventory snapshot and a hash-chained history that shows the list was kept current.

Lifecycle with proof

Purchase, assignment, reassignment, repair and disposal are recorded, with sanitization evidence required at the end.

Where it fits

- Works fully standalone, including for non-regulated small businesses
- Syncs assets and posture into Trustivum:Compliance as inventory evidence
- Gives Trustivum:ComplianceDesk the asset behind every ticket
- Supplies scope to, and reconciles discovery from, Trustivum:ComplianceVector

Pricing

Add-on

pricing on request · separate from the Trustivum:Compliance subscription

A proposed update to the HIPAA Security Rule would make a technology asset inventory and network map an explicit requirement. Auditors already ask for both.



Trustivum:ComplianceVector

A policy says what should be true. A test shows what is true. ComplianceVector checks your systems the way an attacker would, then makes sure what it finds gets fixed: a verified finding, a severity, a deadline, a ticket and a retest. Delivered four ways.

MODEL 1 · ONE-TIME

Engagement

\$2,495

flat · limited scope

One external penetration test: up to 3 assets, analyst-verified, control-mapped report, free retest within 30 days, report in 7 business days.

MODEL 2 · SCHEDULED PROGRAM

Scheduled testing

Quarterly

recommended · on request

Baseline engagement, then external scans at your interval: quarterly recommended, or any cadence including on demand. Findings portal and trend report.

MODEL 3 · APPLIANCE

Sentry

Internal

scanning · on request

A compact appliance on your network running scheduled internal scans: discovery, known vulnerabilities, exposed shares. No install, no firewall changes.

MODEL 4 · APPLIANCE

Sentry Pro

Deep

internal · on request

A higher-capacity appliance with a full authenticated scanner on board for credentialed, insider-view assessment. Your data stays inside.

WHAT YOU GET	ENGAGEMENT	SCHEDULED PROGRAM	SENTRY	SENTRY PRO
External testing	Once	At your interval	Add the program	Add the program
Internal network	—	—	Scheduled	Scheduled, credentialed
Analyst verification	Yes	Yes	Yes	Yes
Retest	1 free, 30 days	On request	Next scan	Next scan
Term	One-time	Ongoing, cancel any time	12 months, appliance returned	12 months, appliance returned

Built so the finding gets fixed

- ✓ Every finding verified by a person before it reaches your report
- ✓ Severity with a fix window; critical issues flagged the day they are verified
- ✓ Scope and written authorization on record before anything runs

Where it fits

- Sells standalone to any company that needs a test
- Report lands in Trustivum:Compliance as evidence
- Each finding opens as a ticket in Trustivum:ComplianceDesk
- Discovered hosts reconcile against Trustivum:ComplianceLedger



TRUSTIVUM

Whichever one your auditor circled, start there.

Most teams start with a one-time penetration test or the compliance platform, then add the daily-work tools as they grow. Tell us where you are.

Talk to us

hello@trustivum.com
www.trustivum.com

Request a penetration test

services.trustivum.com/penetration-testing/

A note on language. Trustivum supports SOC 2 and HIPAA readiness. It does not certify companies, and no company is "SOC 2 certified"; an independent auditor issues a SOC 2 report. SOC 2 Type 1 evaluates whether controls are suitably designed and implemented at a point in time. SOC 2 Type 2 evaluates operating effectiveness over a defined review period. There is no HIPAA certification; Trustivum helps a company build and maintain its HIPAA compliance posture. No tool can promise an audit outcome.

Prices shown are current published prices and may change. Add-on pricing is quoted on request.
Trustivum, LLC · Site design and marketing by Mad Monkey Creative.