Vanta vs Drata vs Secureframe: how to actually choose a SOC 2 platform

The three compliance-automation platforms overlap so heavily on features that price is the wrong first question, especially since none of them publish list prices. Here is what actually separates them, and the two cost lines the platform quote never includes.

Published 2026-07-01 · A Mue guide

An enterprise prospect asks for SOC 2, you start comparing platforms, and within an hour every review page has told you a different one is the winner. The reason the comparisons disagree is that the three leading compliance-automation platforms, Vanta, Drata and Secureframe, do broadly the same job to a similar standard. Feature-for-feature they have largely converged, so the real question is not which is best in the abstract, but which fits your team and how well you negotiate the quote.

What all three actually do

Before the differences, the overlap, because it is most of the picture. All three connect to your cloud, identity, code and HR systems, pull evidence on a schedule so you are not screenshotting settings by hand, map that evidence to a framework control set, watch for drift and alert you when a control falls out of compliance, ship policy templates, and give your auditor a portal to review it all. Each covers SOC 2, ISO 27001, HIPAA, GDPR-related controls and a growing list of other frameworks from one control set. If your shortlist is these three, you are not choosing between capable and not capable, you are choosing on fit.

Where they genuinely differ

- Vanta: the broad default. It has the largest integration library and auditor network and the fastest out-of-the-box setup, so it gets a typical SaaS team to a working evidence set with the least effort. If you have no strong reason to pick otherwise, this is the low-friction choice.
- Drata: engineering-first. It leans into deeper automation and tighter CI/CD and infrastructure hooks, which rewards a DevOps-heavy team willing to wire compliance into its pipeline rather than manage it as a separate portal.
- Secureframe: advisory and multi-framework. It bundles more hands-on guidance and broad framework coverage, which suits a team with no internal GRC person who wants the vendor to carry more of the process, and teams running several frameworks at once.

Those are differences of emphasis, not of capability class. A DevOps team can run Vanta and a lean SaaS team can run Drata; the point is which one is pushing with your grain rather than against it.

Why nobody can quote you a price

None of the three publish list prices. Every quote is assembled from your headcount, the frameworks you turn on and which modules you add, so a like-for-like sticker comparison does not exist, and any single number you see online is one company's deal, not a rate card. The reported bands do cluster: for a single-framework SOC 2 at a company under about 50 people, platform fees tend to land somewhere around 7,500 to 15,000 dollars a year across all three, with Drata's entry tier commonly reported around 9,000 to 12,000 and Secureframe currently quoting most aggressively to win startups. Larger headcounts and extra frameworks push all three well above that. (Reported ranges, not official list prices, and they move.)

The practical consequence is that price should be your last filter, not your first. Because the vendors compete directly and none post rates, buyers routinely take a quote from one and use it to negotiate another down 20 to 30 percent. Get at least two quotes, pick the platform that fits your team, and let the competing number do the discounting.

The two lines the platform quote never includes

The most expensive misunderstanding about these tools is assuming the subscription is the cost of your SOC 2. It is not. The platform automates evidence; it does not issue the report.

- The audit is separate. A SOC 2 report can only be issued by an independent licensed CPA firm, which is a different company you engage and pay on top of the platform, roughly 12,000 to 30,000 dollars for a Type II. The platforms have partner auditor networks and hand off cleanly, but the auditor invoice is its own line.
- Implementation is usually its own cost. Getting controls actually in place, and often a required onboarding or implementation package, commonly adds something in the region of 10,000 to 25,000 dollars in year one, plus an independent penetration test that auditors and enterprise buyers expect.

Add the platform fee, the auditor, implementation and your own team's hours together and the software is often the smaller part of the total. Our companion piece on what SOC 2 really costs a startup walks the full four-line breakdown; the takeaway here is to budget the project, not the subscription.

The renewal and lock-in you are signing up for

Two contract mechanics matter as much as the year-one price. First, switching platforms later means re-doing integrations and re-mapping evidence, so once a report is running most teams stay, which is precisely why vendors discount so hard to win year one. Second, renewals commonly rise, with reported increases anywhere from 10 to 50 percent, so the introductory quote is not the price you keep. Treat this like any committed SaaS contract: ask for a renewal cap in writing before you sign, and size the commitment against the frameworks you will actually run, not the ones a demo made you want.

How to decide, in order

- Pick for fit first: Vanta for the broad low-friction default, Drata for an engineering-led team, Secureframe when you want more advisory and multi-framework coverage.

- Get two quotes and negotiate, because none publish rates and a competing quote is your main lever.
- Budget the whole project: platform plus a separate CPA auditor plus implementation plus your team's time, not the subscription alone.
- Get a renewal cap in writing, because the year-one price is discounted and lock-in is real once a report is running.

See your own number

The platform fee is the one line every comparison fixates on and the one that varies least once you negotiate. The lines that actually move your total, the auditor, implementation and your team's hours, are the ones the vendor pages leave out. Put your headcount and framework into the estimator to size the full SOC 2 cost, then treat the platform quote as a negotiable slice of it rather than the price of the whole thing.

Frequently asked questions

Which is cheapest: Vanta, Drata or Secureframe?
There is no fixed answer, because none of the three publish list prices. Every quote is built from your headcount, the frameworks you need and which modules you turn on, so the same company gets three different numbers. Reported bands for a single-framework SOC 2 at a small company cluster around 7,500 to 15,000 dollars a year in platform fees for all three, with Secureframe currently the most aggressive on startup pricing and buyers routinely using one vendor quote to negotiate another down 20 to 30 percent. Treat the platform fee as negotiable, not fixed.

What is the real difference between Vanta, Drata and Secureframe?
Less than the marketing suggests. All three automate the same core job: pull evidence from your stack on a schedule, map it to controls, and give the auditor a portal. The practical differences are emphasis. Vanta has the largest integration library and auditor network and the fastest out-of-the-box setup, which suits most SaaS teams. Drata leans engineering-first with deeper automation and tighter CI/CD hooks, which suits DevOps-heavy teams. Secureframe bundles more hands-on advisory and broad multi-framework coverage, which suits teams with no internal GRC expertise.

Does the platform fee cover the whole SOC 2?
No, and this is the number that surprises founders. The platform automates evidence, but it does not perform the audit. A separate, independent CPA firm writes the SOC 2 report (roughly 12,000 to 30,000 dollars), and most teams also pay a one-time implementation or onboarding cost (often 10,000 to 25,000 dollars) plus an independent penetration test. The platform subscription is one of three or four cost lines, not the total.

Can I switch platforms later, and do prices rise at renewal?
You can switch, but it means re-doing integrations and re-mapping evidence, so most teams stay put once a report is running, which is exactly why vendors discount hard in year one. Renewals commonly rise (reported increases run anywhere from 10 to 50 percent), so the year-one quote is not the price you keep. Ask for a renewal cap in writing before you sign, the same

discipline the Salesforce and enterprise-SaaS contracts need.

Do these platforms handle ISO 27001 and other frameworks too?
Yes. All three map one control set to multiple frameworks, so SOC 2, ISO 27001, HIPAA and GDPR-related controls largely reuse the same evidence rather than doubling the work. If you expect to need more than one framework, multi-framework coverage and how each vendor prices the second framework matter more than the single-framework sticker.

Estimate your full SOC 2 cost, not just the platform

Free, no signup: agent.mue.app/tools/soc2-iso27001-readiness-cost-estimator

agent.mue.app/articles/vanta-vs-drata-vs-secureframe-which-soc2-platform