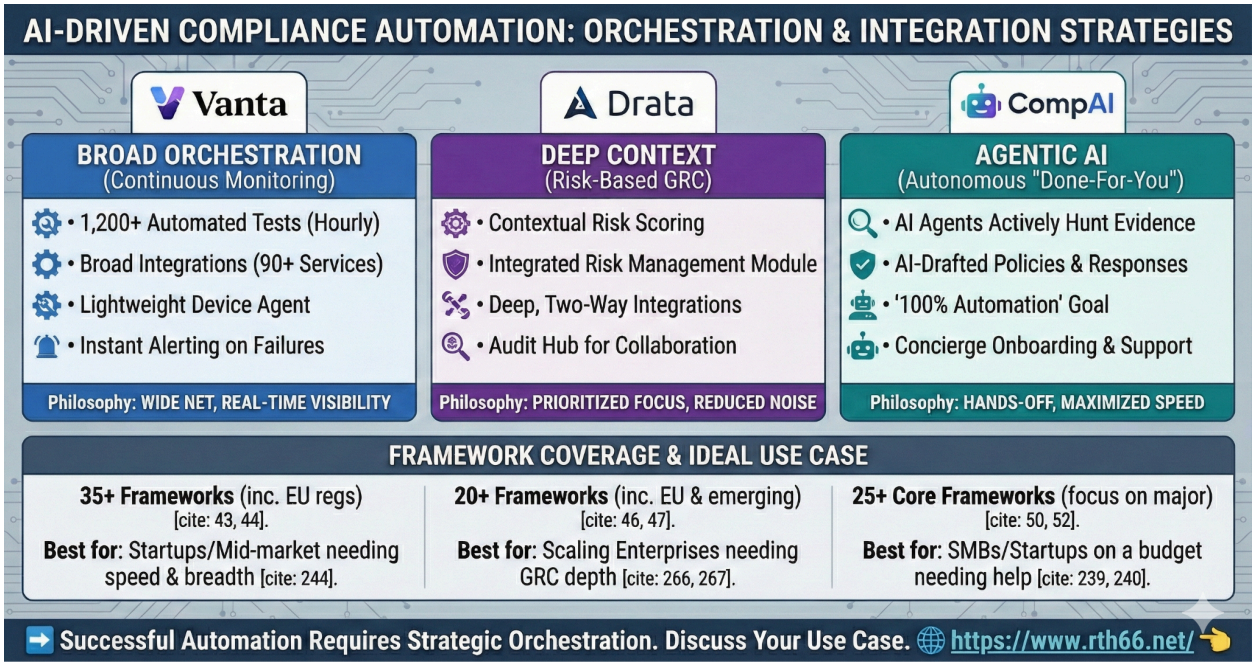

Comparative Analysis: Vanta vs Drata vs CompAI – AI-Driven Compliance Management Tools

Overview of the Platforms

Vanta, Drata, and CompAI are leading AI-driven compliance management platforms designed to streamline the process of achieving and maintaining security certifications and regulatory compliance. All three platforms automate evidence collection, monitor controls continuously, and provide centralized dashboards for multiple frameworks. However, they differ in feature depth, supported standards, approach to automation, and target audience. Below we compare their **functions**, **supported frameworks/certifications**, **automation integrations**, **feature sets (templates, trust centers, etc.)**, **pricing models**, and **ideal use-cases**. We also incorporate **customer feedback**, highlight **limitations/risks**, and give recommendations for each specific scenario.

Core Functions & Automation Features

All three tools automate core compliance tasks, but with different emphases:

- **Automated Evidence Collection:** Each platform integrates with cloud services and IT tools to gather proof of controls in place. **Vanta** touts **1,200+ automated tests running hourly** across a broad ecosystem of integrations[1][2]. For example, if MFA is disabled on an account or a laptop is unencrypted, Vanta will flag it quickly (Vanta's agent runs frequent checks)[3][4]. **Drata** also continuously monitors controls but takes a risk-based approach – many checks run daily

(some near real-time) with **contextual risk scoring to reduce noise**, meaning fewer false positives and more prioritization of critical issues[3][5]. **CompAI** uses AI "agents" to actively hunt for evidence (even taking screenshots) across your systems with **100+ out-of-the-box integrations**, similarly auto-documenting your controls[6]. In practice, Vanta casts a wider net of integrations while Drata focuses on deeper automation per integration[7]. CompAI's approach is all-inclusive – it claims **100% automation rate**, aiming to have AI agents complete every evidence-gathering task possible[8].

- **Policy Management & Templates:** All platforms provide pre-mapped controls and policy templates to jump-start compliance. **Vanta** includes a library of **pre-built policy templates** for each framework and a step-by-step policy builder, with tracking for employee policy attestations[9]. **Drata** similarly offers an in-app **Policy Center** – for example, Drata's DORA module comes with *20+ customizable, auditor-approved policies* ready to use[10]. **CompAI** also handles policies with an AI twist: its agents can automatically **generate or update security policies** and customize them for you. In fact, CompAI advertises that its AI continuously researches best practices and **updates your policies** (and even vendor risk profiles) to keep up with new threats[11]. All three tools thereby save you from writing policies from scratch, but CompAI leans into AI to manage this "busywork" for you end-to-end.

- **Risk Management & Security Oversight: Drata** goes beyond basic compliance by including robust **integrated risk management** features. It lets you log and score risks, assign owners and remediation deadlines, map risks to controls, and track third-party (vendor) risks, functioning as a mini GRC solution[12][13]. **Vanta**, historically focused on automated technical checks, has added some risk features (e.g. an access review module for user permissions and integrations with vulnerability scanners for issue tracking) but doesn't yet offer a full risk register with scoring out-of-the-box[14]. **CompAI** emphasizes "AI-powered risk intelligence," meaning the platform will proactively monitor your vendors and environment for emerging risks and suggest mitigations. For example, CompAI's agents can continuously research your third-party providers and update their risk scores automatically[11]. This is a unique angle, potentially alerting you to new vendor security issues without manual effort. In summary, for a formal risk management program Drata currently has the edge, while Vanta covers essential security checks, and CompAI aims to automate even the risk research aspect.

- **Trust Centers & Assurance:** Providing security transparency to customers is another key feature area. **Vanta** and **Drata** both include **Trust Center** portals where you can share your compliance status, reports, and even automatically answer security questionnaires. Drata acquired SafeBase (a popular Trust Center solution), so Drata users can publish a rich trust portal and even leverage **AI-driven questionnaire completion** to answer customer security questionnaires faster[15][16]. Vanta also offers a public-facing Trust Center and recently

introduced **AI-powered questionnaire automation** (available in higher tiers) to handle repetitive security review questions[17][18]. **CompAI** similarly provides a **real-time trust portal** on your own domain, populated with live compliance data. Notably, CompAI advertises *AI-powered questionnaire responses* as well – meaning the platform's AI will draft answers to incoming security questionnaires using your evidence and policies[19]. This feature in all three tools can significantly accelerate sales cycles by quickly addressing customer concerns with up-to-date info.

- **Employee Device and Access Compliance:** Managing end-user devices and accounts is critical for frameworks like SOC 2. **Vanta** includes its own lightweight **agent for device monitoring** – employees install the Vanta agent on their laptops, and it automatically checks for things like disk encryption, OS patch level, password policy, etc. (and can even enforce certain configurations)[20]. This is great for startups or SMBs without an IT department or MDM (Mobile Device Management) system: Vanta will ensure every machine meets security baseline. **Drata**, on the other hand, does *not* use a proprietary agent; instead it **integrates with third-party MDMs** (like Jamf, Kandji, Microsoft InTune, etc.) to pull device compliance data[20][21]. This means Drata fits well if you already have an MDM – it will ingest and show compliance status from those tools – but if you don't, Drata won't directly monitor devices (no Drata agent). Aside from devices, both Vanta and Drata have features for **user access reviews** (periodically reviewing who has access to critical systems) to satisfy compliance requirements. CompAI also supports automated access reviews and goes a step further by promising that its AI agents will *"complete every task"* – implying tasks like onboarding users, offboarding, sending training, etc., are fully automated as well[22]. (CompAI provides built-in security awareness training reminders and tracks completion, similar to its competitors[23].) In summary, Vanta offers more built-in device compliance for those without existing tooling, Drata aligns with companies already using device management solutions, and CompAI attempts to handle everything automatically once configured.

- **Audit Support and Workflow:** All three platforms strive to simplify the audit process itself. **Drata** offers an **Audit Hub** where you can invite your auditor to log in, review evidence mapped to each control, and even have real-time Q&A with you in the platform[24][25]. Many audits can thus be completed inside Drata, reducing back-and-forth emails and file transfers. **Vanta** also allows you to give auditors read-only access to your compliance dashboard and evidence[26]. Auditors familiar with Vanta can navigate the evidence directly, though Vanta's collaboration features are not as elaborate as Drata's (which was built explicitly to streamline auditor interactions). **CompAI**, despite being newer, has a network of **pre-vetted partner auditors** who know the platform. It will connect you with an auditor and claims to *"fast-track your certification process"*, essentially bundling audit facilitation as part of its white-glove service[27]. Furthermore, CompAI is confident enough to offer a **100% audit success guarantee**, advertising a full

refund if you don't pass your audit or aren't satisfied[28] – a bold promise not seen with Vanta or Drata.

Supported Frameworks, Certifications & Regions

One of the most important considerations is whether a tool supports the specific **compliance frameworks or certifications** your organization needs. All three platforms support multiple standards:

- **Vanta:** Vanta has the broadest library, with **35+ security and privacy frameworks supported**[29]. This includes all the common ones – **SOC 2**, **ISO/IEC 27001**, **HIPAA**, **GDPR**, **PCI DSS**, **HITRUST**, **CSA CCM**, **NIST CSF**, **NIST SP 800-53/171**, **Cyber Essentials (UK)**, **Essential Eight (AUS)**, **CJIS**, **CMMC**, etc. – as well as newer and region-specific regulations. Notably, in late 2023 Vanta announced support for emerging **EU regulations like NIS2 and DORA**, as well as the EU AI Act[30][31]. This means Vanta can help European companies comply with the **NIS2 Directive** (new EU cybersecurity requirements) and the **Digital Operational Resilience Act (DORA)** for financial entities, mapping those requirements into the platform. Vanta allows cross-mapping of controls across frameworks, so you can "do the work once" and apply evidence to multiple standards[32]. In short, Vanta is very comprehensive in terms of framework coverage – you can even add custom frameworks if needed[30].

- **Drata:** Drata supports **20+ frameworks** out-of-the-box[33][34]. This includes all major ones similar to Vanta: **SOC 2**, **ISO 27001**, **HIPAA**, **GDPR**, **PCI DSS**, **CCPA (California Privacy)**, **CMMC**, **FedRAMP**, **HITRUST**, **TISAX** (German automotive), **NYDFS** (New York financial cyber rule), **CIS Controls**, **Microsoft SSPA**, and more[35][36]. By 2024, Drata also added support for **NIS2** and **DORA** in its framework lineup[37][38]. In fact, Drata highlights how its platform can accelerate DORA compliance by **cross-mapping DORA requirements to existing ISO 27001/GDPR controls** to save effort[39]. Similarly, Drata has a dedicated module and guidance for NIS2 compliance (ENISA's directive). Drata is quick to incorporate new frameworks (for example, it added **ISO 42001** for AI management and **NIST AI RMF** for AI risk governance as those emerged[40]). If you need a framework that's not pre-loaded, Drata allows creating **custom frameworks** as well[41][42]. Overall, while the sheer number is slightly fewer than Vanta's, Drata covers all widely used standards and keeps up with new regulations in both the US and Europe.

- **CompAI:** As a newer entrant, CompAI also recognizes the need to handle multiple frameworks. It supports **25+ leading compliance frameworks** across info security, data privacy, and AI governance[43]. On its website and Product Hunt launch, CompAI specifically calls out **SOC 2, ISO 27001, HIPAA, GDPR** as core frameworks it makes "effortless"[44]. It undoubtedly covers others like PCI, probably HITRUST, etc., though detailed lists aren't publicly enumerated. The platform is **open-source**, which means the community or CompAI's team can add

new frameworks relatively quickly by defining the control mappings. However, as of now, CompAI's emphasis is on the major four mentioned. It references AI governance frameworks too, implying support (or plans to support) things like **EU AI Act** or **NIST AI RMF** (since Vanta/Drata do). If your compliance needs are mainly SOC 2/ISO/GDPR, CompAI will handle those out of the box. For very niche or emerging frameworks like NIS2 or DORA, CompAI does not yet advertise native support – you might need to manually configure those or use the custom framework feature. In contrast, Vanta and Drata have pre-mapped those EU frameworks already[30][38]. So, for an organization needing a *wide* array of certifications (e.g. a cloud provider requiring SOC 2, ISO27001, **and** FedRAMP, DORA, etc.), Vanta or Drata currently have a more mature library ready to go. CompAI's 25+ count covers the essentials and relies on a generalized mapping approach for others.

Integrations and Level of Automation

Successful compliance automation depends on **integrations with the software stack** your company uses – cloud providers, identity providers, version control, ticketing systems, endpoint management, etc. Here's how the tools compare:

- **Vanta Integrations:** Vanta integrates with **over 90 services** (as of 2025) across cloud infrastructure (AWS, GCP, Azure), DevOps and CI/CD (GitHub, GitLab, Jenkins), HR systems (e.g. BambooHR, Workday), ticketing/project tools (Jira, Asana, ClickUp), security tools (Snyk, Nessus, Cloudflare, etc.), identity providers (Okta, Google Workspace, Azure AD), endpoint management (Jamf, Kandji, etc.), and more[45]. This broad support means Vanta can collect evidence from a wide variety of sources automatically. If your stack includes a less common SaaS tool, there's a good chance Vanta might already have a connector for it (their breadth is a selling point[7]). Vanta's approach is to run frequent checks on these integrations – essentially polling for compliance status roughly **hourly** in many cases[2]. The benefit is near-real-time visibility; the drawback could be a flood of alerts if not tuned, though Vanta provides a live dashboard to watch control status in real time[46].

- **Drata Integrations:** Drata also has **hundreds of integrations** covering all the major categories (cloud, code, HR, security, identity, etc.)[33]. In practice, for any system crucial to compliance, Drata likely supports it – and like Vanta, it has an API to integrate custom systems if needed. One distinction is that Drata emphasizes *depth* of integration. For example, Drata's integrations often allow more granular checks and two-way capabilities: it can not only pull data (e.g. list of AWS resources and configs) but also link to external workflows (like creating Jira tickets for issues or syncing user data via SCIM). Drata tends to do at least daily checks (or faster) and then **prioritize alerts based on risk**[3][47]. Users have noted that Drata's alerts might be less noisy – the platform might wait to flag an issue until it's certain or high-priority, whereas Vanta flags anything failing immediately[48]. Both strategies have merit: Vanta gives you instant insight,

Drata reduces false alarms. Unless your stack involves a very unusual tool, both Vanta and Drata will cover your needs. (If you have an entirely on-prem system, Drata can even integrate via agents or API, whereas Vanta's focus is more cloud/SaaS – but both have solutions for on-prem evidence by manual input if needed[49].)

- **CompAI Integrations:** CompAI lists **100+ integrations** which, while fewer than the big two, likely cover the most commonly used services for startups (AWS, GitHub, Azure, Google, Okta, Jira, Slack, etc.)[6]. Since CompAI is open source, if a connector is missing, technically a development team could create one or use community contributions. The platform's philosophy is to automate evidence gathering as much as possible via these integrations and AI. For example, not only will it connect to your AWS account to check configurations, but its AI might *take screenshots* of configurations or reports for evidence[6] – something traditional tools usually don't do unless explicitly configured. This can be helpful for auditors who like visual evidence or when an API doesn't provide a certain piece of proof. Being a newer platform, CompAI may not have integrations for extremely legacy or enterprise-specific systems yet, but it focuses on the typical modern SaaS stack used by cloud companies. If your organization uses standard tools, CompAI should integrate smoothly; if you have a very bespoke environment, you'd either need to extend CompAI or lean on the others.

In summary, **Vanta offers the widest integration support**, **Drata offers depth and intelligent monitoring**, and **CompAI covers the basics with the ability to extend via open source**. All three will automate away a huge chunk of manual evidence collection – connecting to your systems to pull logs, user lists, config settings, and so forth – which is a core reason to use them. Just ensure whichever you choose can plug into all critical systems you have (always check their integrations list), and note that **Vanta's built-in laptop agent is a unique integration point** for endpoint data if you lack other device management[20].

Additional Features & Support Resources

Beyond core compliance checks, there are other features and support offerings that differentiate these tools:

- **Employee Training & Personnel Management:** To satisfy requirements for security awareness training and background checks, **Vanta** provides built-in solutions. Vanta includes **out-of-the-box security awareness training videos** and tracks if employees have completed them, as well as options for running background checks through the platform[50]. It also has onboarding/offboarding workflows to ensure new hires sign the policies, install agents, etc. **Drata** likewise offers an integrated training module – e.g. in the DORA framework Drata provides, it highlights that you can automate sending training reminders and record completion within Drata[23]. Both platforms thus cover the human side of compliance (you get dashboards of which employees have accepted policies and

finished training). **CompAI** hasn't explicitly advertised training content, but given its "100% automation" ethos, it likely partners or allows integration to ensure those tasks are done (or one could integrate a training SaaS via CompAI). In any case, neither Vanta nor Drata require you to procure a separate training tracking system for compliance – it's included, which is a big convenience.

- **Pre-Built Controls and Cross-Mapping:** All three tools come with extensive **control libraries**. For instance, Vanta provides a set of **pre-built controls** for each supported framework, which you can adopt or customize[51]. Drata similarly has a **built-in controls and requirements library**, so you're not writing control statements from scratch – you select from standard controls aligned to SOC 2, ISO 27001, etc.[52]. These controls are often cross-mapped across frameworks: **Drata's control mapping** means evidence for one framework can satisfy another (for example, a strong password policy control can map to SOC 2, ISO, PCI simultaneously)[33][53]. Vanta explicitly allows cross-mapping as well, avoiding duplicate work[32]. **CompAI** being open, likely leverages common control mappings too (and their blog notes intelligent control mapping to prevent duplicating effort when adding frameworks[54]). This is important for companies pursuing multiple certifications – the platforms ensure you don't have to implement separate silos of controls for each standard; instead you implement once and comply with many.

- **Customer Support and Guidance: Drata and Vanta both have high customer satisfaction ratings for support**, but Drata is especially praised for its **real-time chat support**. On G2 (a software review site), Drata scores **9.6/10 for Quality of Support vs Vanta's 9.0**[55]. Users report that Drata has a chat box within the app and response times of 2–3 minutes from knowledgeable compliance experts[56][57]. Vanta's support is also well-regarded (9.0 is a strong score) and they have a large help center and community, but their model is usually **ticket or email-based support rather than live chat**[58]. Depending on your preference, this can matter – small teams often love Drata's instantaneous help for questions during audit prep, whereas others may not mind waiting a bit for an answer via Vanta's support. **CompAI** being a newer company, positions itself as very high-touch: they provide **1:1 Slack channel support with a 5-minute response SLA** for customers[59]. Essentially, CompAI promises an experience where you get a dedicated success manager on Slack answering in real-time (mirroring white-glove consultancy). This is part of their "done-for-you" approach, and can be a huge benefit if you're not well-versed in compliance – they will practically hold your hand through the process. In summary, all three prioritize customer success, but Drata and CompAI offer *interactive, real-time support channels* that many customers find invaluable, whereas Vanta's support, while effective, is less instantaneous.

- **Ease of Use vs. Flexibility:** Both Vanta and Drata are considered user-friendly, but there are slight differences. **Vanta's interface** is often praised for being **clean**

and straightforward, with a clear checklist of tasks and progress bars (e.g. “75% of controls passing”) that non-technical founders can easily follow[60]. It doesn’t overwhelm the user with too many menus. Drata’s UI is also modern and intuitive, but **because Drata offers more modules (risk, vendor management, etc.)**, there are naturally more sections and settings which can feel a bit more complex at first[61]. In fact, G2 reviewers rate Drata’s *ease of use* at 9.1 vs Vanta’s 8.9 – essentially tied[62]. Drata’s onboarding is very structured (a guided sequence to connect integrations, select frameworks, generate policies, etc.) which can get a company up and running in as little as a day[63][64]. Vanta also uses checklists for onboarding but gives the user a bit more freedom to navigate in different orders. Ultimately, both are quite polished; Vanta might have a slight edge for first-time users with its minimalism, while Drata provides more *power-user* depth once you learn it. **CompAI**, in contrast, is aiming to eliminate complexity entirely by doing most of the work for you – it advertises “audit-ready in hours” with **CompAI handling the entire setup** and configuration on your behalf[65][66]. This suggests that CompAI’s team will actually configure integrations, customize policies, etc. for you as part of onboarding (white-glove service). The trade-off is you rely on their experts, but for many small companies that’s a plus. The UI of CompAI is less battle-tested (and being open-source, it’s evolving), but their value prop is you shouldn’t need to spend much time in the UI at all – they’ll get everything in place very quickly (as evidenced by a customer quote: *“We were only 30-40% through SOC 2 with Vanta after 4 months. We switched to CompAI, and they had us audit-ready in a couple of days.”*[67]).

- **Ecosystem and Partners:** Vanta and Drata both have extensive **partner networks**. Vanta provides directories of recommended consultants and auditors who are familiar with the platform[68][69]. They also have recently expanded into adjacent areas (for example, Vanta acquired a third-party risk management startup to bolster vendor risk capabilities[70][71]). Drata has partnerships with many audit firms and even distributors in various regions (like a partnership with Distology in Europe) – showing they are building a channel to reach more customers[72]. For a customer, this means whichever tool you choose, you can likely find external help (consultants or auditors) who know that tool well. CompAI, being new, has fewer formal partners, but as mentioned, they maintain relationships with auditors who “know CompAI” to ensure smooth audits[27]. Over time, if CompAI grows, its ecosystem will too – but currently Vanta and Drata have the larger communities and third-party resources (e.g. many blogs, user communities, etc., exist for them).

Pricing and Licensing Models

Pricing is often a deciding factor, and there are notable differences here:

- **Vanta Pricing:** Vanta does not publish fixed prices on its site; it uses a customized quote model based on factors like company size (number of employees or devices), number of frameworks, and add-on features needed. Industry data and

customer reports indicate **Vanta starts around \$10,000 per year** for a basic single-framework package[73][74]. That "Core" or Essentials plan (one framework, up to ~20-50 employees) includes the core automation, one trust report, etc. As you grow, costs increase. The next tier (Plus/Growth) can range roughly **\$15,000–\$30,000/year** for mid-sized teams wanting multiple frameworks or more features[75][76]. Vanta's higher tiers (Scale/Enterprise) with advanced functionality (custom tests, advanced integrations, priority support) can go from **\$30k up to \$80k+ annually** for large companies[77][78]. Additionally, Vanta tends to charge more if you add frameworks – e.g. adding ISO 27001 or HIPAA on top of SOC 2 will raise the subscription. There can also be **hidden costs**: for instance, automated security questionnaire packs beyond a certain number, or SCIM user provisioning capability, are only in higher-cost plans[79][80]. And remember, the auditor's fee is separate (an actual SOC 2 audit by a CPA firm might cost ~\$20k itself, not paid to Vanta). **License model:** Vanta's contracts are typically annual subscriptions. Many startups join via referrals or accelerators which sometimes give discounts for the first year[81], but expect renewal costs to possibly increase after year one. In short, Vanta is a significant investment (their own marketing positions it as replacing the need for large in-house compliance teams). For what it's worth, Vanta's pricing is comparable to hiring one security analyst – many companies find the ROI acceptable given the time saved, but for very small budgets it can be steep.

- **Drata Pricing:** Drata similarly keeps pricing opaque and custom-quoted, but reports suggest it's slightly more accessible for small companies. The **Drata "Foundation" plan starts around \$7,500–\$10,000 per year** for up to 50 employees and one framework[74][82]. This includes basic automation and integrations for, say, SOC 2. The next tier, **Advanced, might run \$15k–\$25k/year** depending on headcount and if you add a second framework[83]. Drata's Enterprise plans (unlimited frameworks, multi-entity support, advanced modules) range broadly but can easily be **\$50k+ to \$100k/year** for large scale organizations[84]. On average, real Drata customers report about \$30k–\$40k/year spend for mid-sized usage[85]. Like Vanta, Drata's cost scales with number of employees and frameworks: as you grow or need HIPAA, PCI, etc., you pay more. Also, features like additional questionnaires, advanced risk management, or API access might be reserved for higher tiers (for example, open API and unlimited users come in the Advanced tier and above)[86]. **License model:** Drata is also sold as an annual SaaS subscription. One difference is that Drata has been known to offer a **monthly payment option** via AWS Marketplace for startups (for instance, \$625/month for the base plan via AWS)[74] – which can help cash flow, though the commitment is essentially the same. Neither Drata nor Vanta's base price include the auditor/certification fee. Both may have occasional promotions (Drata has partnered with investors and incubators to give startups slight discounts or extended trials, just as Vanta has). Overall, Drata's **starting price is a bit lower than Vanta's** (by a couple thousand dollars), but at

scale both end up in the tens-of-thousands annually. Both are **premium solutions** in this market.

- **CompAI Pricing:** CompAI is designed to be a **cost-disruptive alternative**. It offers a dual model: you can use the **open-source software for free** (self-host it on your own servers), or opt for CompAI's **hosted/managed service which starts as low as \$3,000** total[87]. Importantly, CompAI does **not require an annual contract** – you could pay month-to-month, which is unusual in this space[87]. The founders have stated their goal is to shift costs to the end (the audit) rather than charging huge upfront subscriptions[88][89]. In practice, this means a startup could potentially use CompAI to get compliant and only pay a few thousand (plus the auditor fee) instead of \$10k+ for other platforms. Even CompAI's higher-touch packages (with the full white-glove service) are cited in the range of **\$8k–\$15k** – which is still on the lower end relative to equivalently featured plans of Vanta/Drata[90][91]. There are **no hidden add-on fees** for things like extra integrations or users; CompAI's approach is more all-inclusive (they even guarantee success or money back). This pricing strategy is extremely attractive to small businesses and nonprofits that find Vanta/Drata cost-prohibitive[92][93]. The obvious trade-off is that CompAI is a newer platform and company (pre-seed funded), so larger enterprises might be hesitant despite the savings. But for SMBs that can't afford five-figure SaaS bills, CompAI offers a viable path to compliance on a budget.

In summary, **Vanta and Drata are premium, enterprise-grade SaaS with pricing to match (low five-figures and up per year), whereas CompAI aims to democratize compliance with open-source and low-cost plans (in the thousands of dollars)**. If cost is your primary concern and you have some technical ability to self-host or are comfortable with a very new vendor, CompAI is the most budget-friendly by far[93][87]. If you value a long track record, rich features and can allocate a bigger budget, Vanta or Drata will deliver comprehensive solutions (and potentially faster ROI for scaling companies, despite the higher upfront cost). It's worth noting that all three platforms can save money indirectly by reducing audit prep time and helping close sales deals faster – so many companies view them as an investment in growth.

User Feedback: Positives & Negatives

Real-world customer experience with these tools has been largely positive, but there are some differences in focus:

- **Customer Satisfaction:** Both Vanta and Drata have high ratings on review platforms like G2 and Capterra (generally 4.7–4.8 out of 5). **Drata often earns slightly higher marks for support and ease of setup**, as mentioned earlier[62][94]. Users frequently commend Drata's **responsive support team** and the sense that "they are with you" during the compliance journey[57]. Vanta's customers love the clean UI and how much time it saves – many report being able to get SOC 2 in a fraction of the time it would take manually. One user review noted *"Vanta has*

worked great for us! We got through our SOC 2 with no exceptions." (indicating a successful audit) – reflecting the general sentiment that Vanta delivers on its promises. Meanwhile, **CompAI being newer has fewer public reviews**, but the ones available (e.g. on Product Hunt and LinkedIn) are enthusiastic about its speed and service. The **testimonial from Persona (an AI startup)** that after months of slow progress with another tool they became audit-ready in days with CompAI is striking[67]. Of course, such rapid results may not be typical for everyone, but it highlights CompAI's hands-on approach resonating with time-crunched teams.

- **User Experience & Learning Curve: Vanta** is often lauded for its simplicity – "opinionated" in a good way. Non-security professionals (like startup CEOs or CTOs) find it approachable: the tasks are clearly laid out and it integrates seamlessly with engineering workflows (for example, developers get notifications if a GitHub repo is out of compliance, etc.). A minor criticism some have is that Vanta's interface, with its common control mapping, can sometimes feel a bit abstract – new users might not immediately understand how a failing test maps to a specific framework control without some clicking around. Also, Vanta tends to open new browser windows for detailed views, which a few users found confusing[95]. **Drata** users often mention the platform feels very **modern and slick**, and once you connect things, it's clear what to do next thanks to the structured checklist[96]. However, because Drata has many features, some first-time users felt a *slight* **learning curve** finding certain settings or understanding the full range of capabilities[61]. This is usually resolved after a bit of exploration or with help from Drata's support. Overall, both are considered easy to use (nearly equal in ratings). CompAI's UX feedback is not widely documented yet; given their "let us do it for you" model, one could infer the UX is less critical because customers aren't spending as much time configuring things themselves. That said, CompAI's dashboard presumably has similar elements (showing compliance status, controls passing/failing, etc.), and since it's newer, it may still be evolving based on user input.

- **Notable Strengths:**
  Drata – Customers appreciate that Drata is an **"all-in-one GRC platform"**, not just an audit checklist tool. The addition of risk management and vendor risk modules means companies can consolidate more of their governance workflows into Drata instead of using separate spreadsheets or tools. Drata's **AI features for questionnaires** also get praise; several users have noted how much time the automated questionnaire answers save them when responding to prospects' security inquiries (a tedious task for SaaS companies). Another Drata strength is its **Audit Hub and collaboration** – auditors familiar with Drata can perform audits faster, and some audit firms even recommend clients use Drata for the efficiency gains. Drata's investment in **new frameworks (like support for DORA, NIS2)** has been positively received by European customers, as it shows Drata is keeping up with regulatory trends.

Vanta – Customers often highlight Vanta's **breadth of integrations and continuous monitoring**. The fact that Vanta catches issues immediately ("no surprises") is valuable. For example, one might get an alert the same day a developer changes a setting that breaks a control, allowing a quick fix before an auditor ever notices[4]. Vanta's **device agent** is seen as a plus for companies without existing device management – one security engineer mentioned that Vanta "helped us enforce endpoint security across our remote team without needing another tool." Vanta's policy templates and generator (recently enhanced with AI) are also a strong point – many users who aren't policy experts have found it very easy to generate customized policies that satisfy auditors[9]. And while Drata often touts support, Vanta's support is described as **knowledgeable and helpful** too – they just use a ticket system which some actually prefer for tracking purposes.
CompAI – The biggest positive unique to CompAI is **cost and speed**. Early adopters are excited about getting a fully managed compliance service for a fraction of the cost. Some have also noted it's reassuring to have **Slack access to a compliance expert** who basically runs the project for you. Since CompAI can be self-hosted, a few more technical teams like the control that gives them (they can inspect the code, ensure data stays in their own cloud if they want, etc.). Additionally, CompAI's promise of a **money-back guarantee** removes some risk – if it doesn't work out, you could get your fees returned[28]. This is a novel approach in compliance software, showing they are confident in success.

- **Common Criticisms / Limitations Noted by Users:**
  For **Vanta**, one critique that emerges is from some **audit firms** – there are anecdotes that *"auditors have mixed reviews on Vanta."*[97] This often boils down to how Vanta presents evidence. Vanta, in pursuit of automation, sometimes marks controls as "pass" with a green check based on continuous tests, which is great, but certain auditors still ask for additional screenshots or documentation outside of Vanta. In other words, not all auditors fully rely on Vanta's automated evidence, which can frustrate customers who expected the tool to handle everything. This isn't a deal-breaker (most auditors accept Vanta's evidence, especially those in Vanta's network), but it's a point to be aware of – **auditor preferences can introduce hiccups** with any tool. Some users also mention that if you have very custom controls, mapping them in Vanta's framework can be a bit of work (though Vanta's newer AI mapping aims to ease that[51]).
  For **Drata**, a recurring con is its **lack of pricing transparency** (same for Vanta) – prospective customers sometimes vent that they wish pricing was just published or more straightforward. Also, a few users on forums have mentioned *"Drata may require more commitment from engineering teams"*, meaning you might need to involve your engineers a bit to integrate everything properly and to maintain the compliance tasks[98]. This could be because Drata's thoroughness (and risk-based approach) might require fixing a lot of small issues in code repos, tickets, etc., which is ultimately good but can feel like extra work initially. Another noted limitation: since Drata doesn't have its own device agent, if a company had no device management at all, they might have a blind spot (though this is

solvable by adopting an MDM or using manual processes). Generally, **Drata's cons are few**, with the major one being cost for small orgs (just like Vanta) and the complexity of certain advanced features (which only matters if you use them). For **CompAI**, the potential negatives are more about being new: it's less proven at scale, and being open-source, you might wonder about long-term support (though the company has funding now). If you self-host, you take on the operational responsibility (managed hosting from CompAI avoids that but then you're trusting a very young provider). There's also the factor that **CompAI's framework support, while growing, isn't as battle-tested** – if you needed, say, FedRAMP, you'd likely be on your own to configure a lot in CompAI, whereas Vanta/Drata have known playbooks for it. Additionally, by leaning heavily on AI and automation, **CompAI could face hiccups (AI errors)** – one must still review what the AI does. For instance, if the AI drafts a policy or answers a questionnaire, you need to ensure it's accurate and not just plausible-sounding (CompAI's team claims high accuracy, but oversight is always wise). Basically, early adopters carry a bit of risk until CompAI builds a track record.

- **Limitations Observed:** No platform can entirely eliminate the work of compliance. A **critical reality** shared by experienced users is that you will still need to put in some effort to remediate issues and uphold policies. As one guide noted: even with the most automated system, *"you still need to fix security gaps, review policies, complete training, and coordinate with auditors"* – expecting zero effort is unrealistic[99]. These tools will tell you what to fix and even how to fix it (and CompAI/Drata might help do it), but **actual security improvements (like enabling a setting or changing a process) require management commitment**. Another inherent limitation is the **SOC 2 Type II timeline**: no matter how fast you get "audit-ready," you cannot skip the 3-6 month observation period for a Type II audit[100]. Some teams felt disappointed when a vendor advertised "Type II in 14 days" – what that really meant was ready to start the audit in 14 days, then you still need 3+ months of evidence collection for the official report. So, managing expectations is key: these tools speed up readiness and maintenance, but they don't bend time or regulatory rules.

In aggregate, **customer feedback is very positive for all three**. Drata and Vanta have proven their value to thousands of companies (reflected in large customer bases and high retention). CompAI's early customers highlight outcomes like extreme speed and cost-effectiveness, which, if broadly replicated, bode well for its future. The choice often comes down to your company's size, resources, and specific needs – which we'll address in the recommendations.

Key Differences Summary (Pros & Cons)

Before recommendations, here's a quick summary of strengths and weaknesses:

- **Vanta – Pros:** Extremely broad framework support (35+ including latest EU regs)[30]; very frequent automated checks for immediate visibility[3]; wide

integration library (likely to support any tool you use)[7]; built-in device monitoring agent (great for SMB IT basics)[20]; straightforward UI and guided checklists (easy for beginners)[60]; robust policy/template library and new AI features (policy generator, questionnaire automation)[101][17]. Backed by a mature company with ~7,500 customers and high trust in market[102][103].
Cons: Higher starting cost (often \$10k+); support is good but not live-chat; risk management features not as in-depth (may need separate risk tools for advanced use)[14]; some auditors may still ask for evidence outside Vanta in certain cases (so you might not eliminate *all* manual auditor interactions). Vanta's heavy automation can produce lots of alerts – which is proactive, but could overwhelm very small teams until they adjust (some prefer Drata's risk-based filtering to reduce alert fatigue[48]). Overall, few functional cons – mostly cost and the need to fine-tune alerts/processes to your environment.

- **Drata – Pros:** Comprehensive platform that goes beyond compliance into risk and governance (one-stop shop)[12]; strong support (real-time chat, very high satisfaction)[55][104]; covers all major frameworks and kept pace with new ones like NIS2/DORA quickly[38]; provides advanced features like Audit Hub for collaborating with auditors in-app[24]; highly flexible (custom controls, API, on-prem integrations) – suitable from startup to enterprise; fewer false positives and more context due to risk-based continuous monitoring[47][5]; polished UI and structured onboarding for quick setup[96]. Pricing slightly friendlier at the low end (starts ~$7.5k).
  Cons: Still a significant cost for small companies (not "cheap" by any means) and pricing isn't transparent upfront; if you don't have certain IT basics (like an MDM for devices), you might need to implement those alongside Drata; the richer feature set means a tad more complexity – small teams solely focused on just getting a SOC 2 might find some parts of Drata they don't use (risk module, etc.) although you can simply ignore those sections. One could argue Drata's focus on risk and flexibility might require more internal engagement (i.e. you should have someone to leverage those features, otherwise they're underutilized). But real "cons" are few – mostly about scope and cost.

- **CompAI – Pros:** By far the most **cost-effective** option (free self-hosted or low-cost hosted)[87]; offers **white-glove onboarding and support** (they do the heavy lifting, ideal for teams with no compliance expertise)[105]; extremely fast time-to-compliance in their case studies (measured in days or weeks, thanks to AI and expert help)[106][107]; open-source model provides transparency and no vendor lock-in (you have the code and can modify if needed)[108]; AI agents automate not just technical checks but documentation and even proactive risk research[11]; money-back guarantee de-risks trying it[28]. In short, CompAI's proposition is compliance *as a service* with AI – ideal for those who want to outsource the headache but keep control via an open platform.
  Cons: New and relatively unproven – lacks the track record of Vanta/Drata (which some execs or auditors might view cautiously until CompAI is more established);

supports all common frameworks but may require more manual custom work for niche ones (no large user community yet to share custom templates for, say, very specific standards); since it leans heavily on AI, there's a need to double-check AI outputs for accuracy (the team says they review/human-verify, but it's a developing area)[109]. If self-hosting, you need DevOps resources to deploy and maintain the app (the open-source repo). And while the cost is low, you still have to pay for the audit itself in the end – so ensure you budget for a certified auditor (CompAI will connect you, but that auditor fee can be similar regardless of platform). In summary, CompAI introduces some operational and adoption risk simply by being the newcomer, but the upside (especially on cost) is substantial.

With these differences in mind, we can now recommend which tool fits best for specific scenarios:

Recommendations for Specific Use-Cases

1. Small and Medium Business (SMB): For startups or SMBs (say, <250 employees) seeking their first compliance certification (e.g. SOC 2 or ISO 27001) on a limited budget, **CompAI is a very attractive choice**. Its affordable pricing (starting ~$3k, no long contract) and hands-on assistance can enable even a tiny team to achieve compliance[87][105]. You effectively get a virtual compliance officer via CompAI's AI agents and Slack support, which is ideal if you don't have in-house security expertise. If budget is *extremely* tight (non-profit or seed-stage startup), the ability to self-host for free and only pay for audit is unrivaled. That said, not every small business is comfortable self-hosting or being an early adopter – some may prefer a mature platform even if it costs more. If you have the budget and want a proven product, **Vanta** or **Drata** are also suitable for SMBs (many of their customers are startups). Vanta is a favorite among fast-growing startups that need quick SOC 2 compliance to unlock sales – it provides a straightforward, guided path and is slightly more *turnkey* for a pure compliance audit use-case. Drata is great for startups that might value the extra features (e.g. if you have a more security-conscious approach and want to instill risk management early on, Drata offers that). Also, consider your IT environment: if you have no device management in place, Vanta's agent can get you up to speed on laptop security easily[20]; if you already use tools like Okta, Jira, Jamf, etc., Drata will integrate smoothly and its live support can help your small team swiftly address any setup issues[56]. In summary, for an SMB on a budget or tight timeline, **CompAI** is recommended due to its cost and concierge-style help (maximizing speed and minimizing workload). For an SMB with a bit more budget that prefers a widely-used platform, choose **Vanta** if you want simplicity and immediate alerts, or **Drata** if you prefer more built-in guidance and anticipate needing additional frameworks soon. *(Notably, both Vanta and Drata have startup discount programs – if you're in an accelerator or similar, check those out, as they can sometimes reduce the first-year cost to make them more SMB-friendly[81].)*

2. All Frameworks in Europe (including NIS2 and DORA): If you require compliance with **multiple European and international frameworks** – for example, ISO 27001 and GDPR

as a baseline, plus the new **EU NIS2 and DORA regulations** – then you need a platform that has those specific mappings and content. **Drata** would be an excellent choice here, as it has explicitly rolled out support for NIS2 and DORA ahead of many others[38][39]. Drata's platform can cross-map requirements between frameworks, which is useful since NIS2 and DORA overlap with controls from ISO27001/GDPR (Drata emphasizes saving time by leveraging existing ISO/GDPR controls to meet DORA)[39]. Additionally, Drata's strong risk management module aligns well with the spirit of European regulations (both NIS2 and DORA require robust risk assessment and incident response processes – Drata can help manage and document those[110][111]). **Vanta** is equally capable of handling a broad multi-framework compliance program – it, too, supports NIS2 and DORA as of late 2023[30]. Vanta could be used to manage all these frameworks in one dashboard, mapping controls and monitoring continuously. The decision might come down to organizational preference: Drata's approach may suit a company that wants a comprehensive GRC solution (covering vendor risk, issues management, etc., in addition to compliance checks), whereas Vanta is slightly more focused on the audit-readiness and technical controls monitoring. One consideration is **data residency and regional support**: European companies might prefer vendors who store data in the EU. Drata has noted the importance of **EU data hosting** and has been working on that[72], and it has an office in London and partnerships in EMEA. Vanta also opened a London office and has been courting European clients[112]. Both should be fine for European use, but double-check where your data will reside when using their SaaS (as of now, it may still be primarily in the US unless otherwise requested). **CompAI** could be used for European frameworks as well, but since it hasn't published native NIS2/DORA content, you'd likely have to manually implement those controls in CompAI. If you have strong in-house compliance knowledge, this is doable; otherwise, Drata/Vanta provide more out-of-the-box guidance for new EU laws. Given the complexity of managing "all frameworks in Europe," **Drata** might get a slight nod due to its integrated risk management and specific focus on these new directives (it provides FAQ and best-practice content for NIS2/DORA compliance) – making it a one-stop solution for a pan-European compliance strategy. But Vanta is a close runner-up that will also serve well, especially if you prefer its continuous control emphasis. In summary: **for comprehensive EU-focused compliance programs, Drata's multi-framework and risk capabilities are highly recommended**, with Vanta as an equally strong option if its style better fits your team. CompAI would be a secondary consideration here unless budget is a major constraint or you plan to self-host (in which case, you could tailor CompAI to EU needs but with more manual effort).

3. Hyperscalers and Large SaaS Cloud Providers (e.g. SAP, Salesforce, ServiceNow): Large-scale cloud enterprises have vast compliance obligations – not just SOC 2/ISO, but often SOC 1, SOX, regional certs, and perhaps **FedRAMP, DOD SRG, or industry-specific regs**. They also typically operate in complex environments (multiple cloud accounts, on-prem data centers, thousands of employees and assets). For such scenarios, **Drata** is generally the better fit among these tools. Drata's **Enterprise plan** supports multiple entities (for a company with many subsidiaries or business units) and offers the greatest flexibility in custom controls, workflows, and API

integrations[84][113]. Drata was designed as an **"AI-native Trust Management"** platform that can scale – it even integrates with on-prem systems via API, allowing a hyperscaler to bring in data from legacy environments[114]. The robust risk management in Drata will appeal to large orgs that have dedicated compliance and risk teams (they can use Drata to centralize their risk register, vendor reviews, etc. instead of using separate GRC software). Also, Drata's track record includes a number of Cloud 100 companies and late-stage tech unicorns as customers[115], indicating it has been proven at scale. **Vanta** is certainly used by some larger companies as well, but Vanta historically targeted the mid-market/upper-mid market. It can handle multiple frameworks and lots of integrations, but certain enterprise needs (like very granular access controls, on-prem agent deployment, custom reporting) might require working with Vanta's team on a case-by-case basis. In fact, Vanta's Enterprise tier is fully custom and can meet advanced needs, but by the time you're at that level, the cost is quite high (well into six figures)[80]. If a hyperscaler already has a mature compliance program, they might find Vanta a bit limiting on the risk side. On the flip side, some enterprises may like Vanta's straightforward approach to continuous monitoring to augment their internal GRC processes – essentially using Vanta as a monitoring tool while handling governance elsewhere. It's worth noting that **extremely large providers (like SAP or Salesforce themselves)** often build their own compliance systems or use big governance platforms (like Archer, ServiceNow GRC). They might use Vanta or Drata for a subset of tasks or certain business units. Between Vanta and Drata, **Drata is more frequently chosen by enterprise customers who want a full-featured platform** that molds to their complex environment (Drata's ability to customize controls and its upcoming features around scaling compliance programs align with that). **CompAI** is not yet an ideal choice for a hyperscaler. While an open-source tool could theoretically be adapted for a large enterprise, CompAI's strength is speed and simplicity, which appeals more to smaller orgs. A hyperscaler likely has dozens of frameworks and thousands of controls – managing that in CompAI (with a small team's support) would be challenging and unproven. Also, big enterprises often have strict security requirements for third-party software; they might be cautious to rely on a very new vendor or open-source project for mission-critical compliance. Thus, for large cloud providers, **Drata is recommended as the top choice**, with **Vanta as a viable alternative** if the enterprise prefers its specific features or already uses it in parts of the organization. Drata's enterprise-scale focus (and its high support ratings which enterprises value) make it well-suited to complex, multi-framework compliance across large, distributed teams.

4. European Companies in General (EU-Based Organizations): If we consider a broader scenario – an organization operating primarily in Europe – a few factors come into play: support for EU standards (covered in #2), data privacy considerations, and local customer support. **Vanta** and **Drata** have both expanded to serve European clients, so you can feel confident using either in Europe. Drata's move to enable **EU data hosting**[72] is a positive sign for GDPR-conscious customers – you could inquire with Drata about hosting your data in their EU region if that's important (to ensure all your compliance evidence and employee data stays within Europe). Vanta's data residency is less public, but with a London office and many EU customers, they likely have pathways

to comply with EU data transfer requirements (they advertise GDPR compliance for themselves[30]). From a functionality standpoint, both cover **EU-focused frameworks like GDPR, NIS2, DORA, and even the EU AI Act**[30]. One slight edge: Drata provides content in its app or help center specifically for EU laws (e.g. detailed guides for NIS2, comparisons between DORA and other frameworks, etc.), which could be beneficial for an EU company navigating those for the first time. **CompAI** can absolutely be used by European companies too – and if you self-host CompAI in Europe (for example on your AWS EU-West servers), you have complete control over data location, which is a big plus for sovereignty. An EU-based SMB that is very cost-sensitive might prefer CompAI self-hosted so that no data leaves their environment at all (this could simplify compliance with things like Schrems II, since you're not sending data to a US-based cloud service). However, keep in mind that if you use CompAI's hosted service, you'd want to ask where they host EU customer data (they might accommodate EU region hosting given their focus on compliance, but it's worth verifying). For **European small/mid businesses**, if budget allows, Drata could be slightly more aligned simply due to its proactive inclusion of EU requirements and its local partner presence (through Distology and others) which means sales and support might operate in EU time zones. Vanta is equally capable for EU standards and is a great choice especially if you're focusing on technical security compliance (SOC 2, ISO) plus GDPR. So, the recommendation here is nuanced: if you're an **EU company that prioritizes data residency and being on the cutting edge of EU laws**, **Drata** might be the better fit given its explicit EU hosting and rapid adoption of EU frameworks[72]. If you are an **EU-based tech company primarily concerned with international standards (ISO, SOC2) and want a proven simple solution**, **Vanta** works wonderfully – many EU startups (e.g. in fintech and SaaS) have used Vanta to quickly meet international security standards and Vanta's GDPR module will help with privacy compliance too. And if you're an **EU small business or startup with a tiny budget**, **CompAI** is very appealing – plus no worries about US data access if you self-host in Europe. To summarize: European organizations have all three options open; **Drata** gets a slight recommendation for being very EU-aware in its offerings, **Vanta** is a strong option for general security compliance needs in EU (with the company itself showing commitment to Europe via offices and EU-specific features[31]), and **CompAI** is an option for those who want low cost and control (just ensure your audit firm is comfortable with it – many EU auditors may not have seen CompAI yet, whereas they likely have seen Vanta or Drata).

Conclusion & Final Thoughts: All three platforms – **Vanta, Drata, and CompAI** – ultimately share the goal of reducing the headache of compliance through automation and intelligent software. **Vanta** shines for its years of refinement in continuous compliance monitoring and broad framework coverage, making it a safe bet for companies that want a reliable, widely-used solution. **Drata** distinguishes itself with an AI-native, end-to-end GRC approach and top-notch customer experience, which suits organizations that want to integrate compliance into their broader risk and trust strategy (and want responsive support along the way). **CompAI** is the newcomer disrupting on

price and speed, ideal for resource-strapped teams or those who want the flexibility of open source with the convenience of AI and expert services.

When choosing, consider your **organization's size, budget, compliance scope, and internal expertise**. A small startup needing SOC 2 yesterday might go with CompAI (to get audit-ready fast with help) or Vanta (for a straightforward proven path), whereas a scaling mid-market company aiming for multiple certifications might lean toward Drata to leverage its multi-framework and risk management strengths. Large enterprises will likely favor Drata or a combination of tools, potentially still using Vanta for technical control monitoring if they already have a separate GRC system. And European companies should ensure whichever vendor they pick understands EU requirements and can meet any data locality needs – which Drata and Vanta both strive to do, and which CompAI can address via self-hosting.

Importantly, whichever tool you choose, remember that **automation doesn't replace good security practices** – it augments them. You'll still need to invest in actually implementing the security controls the software advises (e.g. encrypt those databases, enforce that MFA, train your staff). These platforms will significantly reduce the admin burden of compliance (collecting evidence, mapping controls, tracking tasks), which in turn frees your team to focus on improving security and compliance outcomes. In the end, the "best" tool is the one that fits your use-case and will be consistently used by your team. All three options have delivered successful audits and certifications for companies around the world, so you won't go wrong as long as you align the tool's strengths with your specific needs. Use the above comparisons to guide that alignment, and you'll be well on your way to a smoother, faster compliance journey **– with AI doing the heavy lifting**.

Sources:

- Official Vanta Website – *Product and Pricing Pages*[9][30][1]
- Official Drata Website – *Product Pages and Framework Support*[116][37][39][12]
- CompAI Website and Blog – *Features, Pricing, and Comparisons*[44][87][55][20]
- Third-Party Analyses – *ComplyJet and LinkedIn articles on pricing, Reddit user feedback*[74][117][88][58]

[1] [9] [29] [32] [45] [50] [51] [68] [69] [70] [71] Compliance automation software | Vanta

https://www.vanta.com/products/automated-compliance

[2] [3] [4] [5] [7] [12] [13] [14] [20] [21] [24] [25] [26] [46] [47] [48] [55] [56] [58] [60] [61] [62] [94] [95] [104] Vanta vs Drata: Complete Comparison (2025) - Comp AI

https://trycomp.ai/vanta-vs-drata

[6] [8] [11] [19] [22] [27] [28] [43] [44] [59] [65] [66] [67] [106] [107] Comp AI - SOC 2 - HIPAA - GDPR - ISO 27001 made effortless

https://trycomp.ai/

[10] [23] [39] [110] [111] DORA Compliance

https://drata.com/product/dora-compliance

[15] [16] [49] [114] [115] [116] Drata - Modern GRC, Compliance & Trust Automation

https://drata.com/

[17] [18] [30] [101] Plans and Pricing

https://www.vanta.com/pricing

[31] [112] New frameworks and updates to help European companies achieve ...

https://www.vanta.com/resources/european-momentum-new-frameworks

[33] [34] [35] [36] [37] [40] [41] [42] [52] [53] Supported Compliance and Privacy Frameworks | Drata

https://drata.com/product

[38] Drata's Post - DORA Compliance - LinkedIn

https://www.linkedin.com/posts/drata_dora-compliance-empowering-financial-institutions-activity-7283511057883480064-7mPe

[54] [87] [90] [91] [99] [100] [105] [109] Compliance Automation Platform: Complete Guide (2025) - Comp AI

https://trycomp.ai/compliance-automation-platform

[57] [97] [117] Drata vs Vanta : r/cybersecurity

https://www.reddit.com/r/cybersecurity/comments/10iz243/drata_vs_vanta/

[63] [64] [96] [102] [103] Vanta vs. Drata - Which Should You Choose?

https://www.planetcompliance.com/grc/vanta-vs-drata/

[72] Drata expands global footprint | Data Centre Solutions

https://datacentre.solutions/news/65260/drata-expands-global-footprint

[73] [75] [76] [77] [79] [80] Vanta Pricing Guide 2025: Real Costs, ROI, and Hidden Fees

https://www.complyjet.com/blog/vanta-pricing-guide-2025

[74] [82] [83] [84] [85] [86] [113] Drata Pricing Plans 2025: Real Cost, Hidden Add-ons & ROI Analysis

https://www.complyjet.com/blog/drata-pricing-plans

[78] [81] [88] [89] [92] [93] Cost-Effective Compliance Automation: Trycomp AI vs Vanta, Drata, Secureframe, and More

https://www.linkedin.com/pulse/cost-effective-compliance-automation-trycomp-ai-vs-vanta-bullock-kdaxe

[98] Drata vs. Vanta: Which Compliance Tool Fits You? - Gralio

https://gralio.ai/compare/drata-vs-vanta

[108] trycompai/comp: AI Native platform to get companies compliant

https://github.com/trycompai/comp