Vanta

by CTO

Compliance Certification

Details

Review Date	10/30/2023
Purchase Date	Q3'23
Implementation Time	1-2 weeks
Product Still in Use	Yes
Purchase Amount	HIPAA and SOC2 for $12k/year
Intent to Renew	95%
Review Source	Elion

Product Rating

Product Overall	4.5
Use Case Fit	5.0
Ease of Use	5.0
API	N/A
Integrations	4.5
Support	4.0
Value	5.0

About the Reviewer

Purchasing Team · User · Implementation Team · Product Oversight

Reviewer Organization

Virtual-First Provider · Behavioral Health

Reviewer Tech Stack

N/A

Other Products Considered

Drata

Summary

- **Product Usage: The product is utilized for compliance with HIPAA and SOC 2 standards, focusing on integrations with the company's specific tech stack.**
- **Strengths: Vanta stands out for its end-to-end nature, providing efficient and streamline processes for achieving compliance, integrating seamlessly with the company's tech stack, and showcasing compliance status to customers.**
- **Weaknesses: The product could benefit from improved FAQs, a proactively scheduled kickoff call with the CSM, and a more human touchpoint approach to support.**
- **Overall Judgment: The reviewer deems Vanta as the correct choice, offering valuable integrations, easy-to-follow processes, proactive support and helping significantly in achieving compliance ahead of company's timeline.**

So today we're chatting about Vanta and how it's used at your company. Before we jump into that, could you give a brief overview of the company and your role there?

Our company focuses on connecting clinicians with self-funded employers to enhance access to mental health care. Currently, our main priorities are achieving HIPAA compliance, expanding our capabilities in care delivery, and obtaining SOC 2 compliance to instill greater customer confidence. I am CTO and cofounder of the company.

What drove you to look for something in the security compliance category?

We'll start working in the care delivery capacity with our first customer in January, so we had a tight timeline. We began looking for solutions in July, and we needed to find and confirm a vendor quickly to kick off compliance work. Our main goal was to achieve HIPAA compliance first, and then work toward achieving SOC 2 Type 1 and Type 2. That was our primary need.

What key requirements did you use to evaluate Vanta and their competitors?

We evaluated the vendors' efficiency, the average timeline for customers to achieve compliance standards, and their pricing. Since we are an early stage company, we wanted to prioritize optimization for price points. Integrations were also important, as we preferred to minimize manual work and have a streamlined process, especially as we began talking to CSMs, and how much guidance they could provide us with becoming compliant. And it was really important that they had experience with our specific technology stack.

Who were some of the vendors that you looked at, and how did they stack up for you?

We evaluated Vanta and Drata. Initially, the first call with both vendors seemed similar, but there was one key factor that set them apart. In terms of cost, both vendors were similar. The timelines for implementation were also comparable. However, Drata did not have as many integrations available for our specific tech stack. Additionally, when we asked about integrating certain aspects, they took longer to get back to us compared to Vanta. The confidence level with Drata wasn't as high as it was with Vanta, who had prior experience working with customers in our type of tech stack. So ultimately, it was this third factor that helped us differentiate between the two.

How did the pricing compare?

I think Drata actually had a slightly lower price, offering a bundle for around $10,500. However, we decided to pay a bit more for Vanta due to their integrations. Additionally, after seeing a product demo, we found that Vanta's user interface was more streamlined and straightforward, which sealed the deal for us.

How did you find the Vanta sales process and product discovery?

The sales process was impressive. Our point person was responsive, proactive, and made us feel like they were on our team, working to get us the best deal. The whole process inspired confidence that they would respond promptly if we had compliance-related questions.

How did you find the onboarding and implementation process?

The onboarding process was straightforward. After my cofounder and I completed the payment, we were invited to create accounts on Vanta. Once we had access, there were helpful tutorial modules that guided us through a pre-configured dashboard of tasks aligned with our specific frameworks. That saved us time and effort in getting everything set up. The integration process went exceptionally well, with clear instructions and smooth setup of all the integrations within just a few hours. Overall, I was impressed with the onboarding and setup process.

What has your workflow been so far with Vanta?

We've wrapped up HIPAA compliance and have made progress on the tasks required for SOC 2, although we haven't gone through the audit yet. We have been introduced to auditors through Vanta.

Our first step was integrating Vanta and setting it up. Then we focused on creating and implementing policies, which was made easier by Vanta's templates. They highlighted the parts that companies typically customize, which saved us time. It would have been helpful to have FAQs specific to each policy, though, since I had a lot of questions that others have probably asked before. Overall, the process was mostly painless. We got the policies approved and submitted them for acceptance within our organization.

Once the policies were in place, we moved on to providing evidence that we complied with the policies. Vanta not only outlines the evidence we need to submit, but also provides separate dashboards for certain types of evidence. For example, there is a risk management dashboard that allows us to track and manage risks within Vanta. This is much more convenient than manually updating an Excel sheet or Google Doc. The access control review dashboard is also helpful for submitting evidence in that area. Having these custom dashboards for specific evidence submissions is a great feature of Vanta.

What would you consider works well, and what is in need of improvement?

I really like the integrations dashboard. It provides a lot of information on things like penetration testing and audits. They have a wide network of professionals to connect you with, so you don't need to look elsewhere. This is great for compliance needs, as Vanta acts as a one-stop shop.

One improvement I would suggest is prioritizing a virtual kickoff call with the CSM. Currently, it's on us to schedule it, and I think having the CSM initiate the call would be beneficial. It helps with introductions and sets the expectation for communication and addressing specific questions. Additionally, the FAQs section could use some improvement, as I mentioned. Apart from that, everything is pretty straightforward.

What are some of the relative strengths and weaknesses of Vanta?

One major strength of Vanta is its end-to-end nature. It provides everything needed for compliance, from submitting proof of requirements to showcasing compliance to customers. Vanta allows for the download or export of reports and even offers a hosted webpage for customers to easily view compliance status. This all-inclusive feature sets it apart from other vendors that lack such capabilities.

However, this end-to-end nature can also be seen as a weakness. It assumes that users can navigate and utilize Vanta without much support from the Vanta team. In reality, first-time users may feel more confident with a couple of calls for clarification rather than relying solely on email communication. While the CSM typically responds promptly via email, it would be beneficial to have the option for phone calls to address broader questions. Despite the strength of an end-to-end solution, prioritizing human touch points is still important.

Can you talk a bit about the dashboard functionality for your customers?

Vanta creates a webpage that summarizes your progress, and you can share it with others via a link. This link allows people to see what you've accomplished so far, even if you're not completely compliant with SOC 2 or another standard. It lets them track your progress and know that you're on the right path. Once you achieve compliance, you'll even get a nice badge to display. This webpage serves as a central place for people to view your status. Instead of sending a PDF report every time there's a change, which can be tedious and time-consuming, it's much simpler to use an automatically updated link. This way, the information is always current and accessible to everyone without cluttering their inboxes.

Did you find any bugs or stability issues with the platform?

I wouldn't say bugs. No stability issues. However, there were some requirements that were not clearly worded at times. They have a section in their dashboard called "tests" that you need to pass. Occasionally, these tests would fail, but there were no clear instructions on how to fix them. It would be helpful if they provided clearer wording and included FAQs or common pitfalls to address these questions and prevent confusion.

What products in your tech stack have you integrated Vanta with, and how did the integration process go?

One example of an integration that was easy for us was the integration with GCP. HIPAA and SOC 2 compliance require that we implement vulnerability scans, which we need to provide evidence of and describe manually. However, with the GCP integration, Vanta automatically recognized that we host our data and backend functions through GCP and also detected our vulnerability scanning feature, automatically submitting evidence of completion. This integration saved us time and provided evidence that I wasn't sure how to find.

Vanta's integrations handle a number of different tasks. For instance, if you need penetration testing or are searching for different integrations, Vanta can be a useful starting point.

And they offered a list of logging vendors that I explored and found more suitable options than the vendor I was already working with. Vanta is a great resource for finding vendors that align with your compliance goals.

Additionally, as we prepare for SOC 2 auditing and aim to complete a Type 1 audit, Vanta's introductions to vendors are very nice. While it can be limiting to rely solely on the vendors they refer, it's a good starting point that provides additional data points for price and service comparison. However, it would be nice to have reviews of the vendors on their platform, as the list is not sorted in any particular way or accompanied by customer feedback, which is understandable.

How have you found the support process?

The response times from Vanta are excellent. I've never had to wait more than 48 hours for a response, and usually it's even faster. The only time it took longer was when they had to consult another team at Vanta. In addition, I find that they're quite open and helpful in their responses. They don't just dismiss my questions with a generic answer. Instead, they provide tailored advice specific to my team's needs. They could just say that it's up to us to figure out what works best for us, but instead they offer insights based on what they've seen other customers do and what they would expect from a company like ours.

Furthermore, Vanta is proactive in reaching out to their customers. When I signed up with them, they asked about my timeline for achieving compliance under specific frameworks. They periodically check in with me to make sure I'm on track to meet my goals. That level of support is really appreciated.

Do you feel like you made the correct assessment going with Vanta?

I think so. I've always been impressed with the product, and the process has been straightforward. We've achieved HIPAA compliance, which was our top priority. We had to reach that goal before January, and it's only October 30, so we managed to do that very quickly.

Do you see any areas for growth for Vanta?

I can't think of anything in particular. Ease, expediency, and being able to keep track of compliance documents over the long term is the goal. Plus, they'll remind you and send you notifications when certain evidence is about to expire or come back to you if you've postponed something. The continuous monitoring is really helpful. So yeah, it has become a mainstay for us, and we plan to keep using it for a long time.

Do you have any advice for buyers who are thinking through HIPAA, SOC 2, HITRUST, or just general compliance?

I think it's important not to underestimate the value of integrations and the user interface of a product. It's not just about looks; it actually makes a difference. There are certain tasks, like policy work and training, that can't be automated and require manual effort, so it's crucial to identify areas where automation can be introduced. Initially, I didn't think having specific integrations mattered much when we were considering signing with Vanta. I believed I could make changes to the stack as needed. However, it would have definitely added to my workload, which was already filled with hours of dealing with policies and network diagrams. These were tasks that couldn't be automated. That's why I really appreciated Vanta's ability to configure settings in my GCP and front-end instances, which helped us achieve HIPAA compliance. So integrations shouldn't be disregarded. Anything that can be automated should be, and the user interface matters.