whistic

The ROI of Transparency

Save time, close deals faster, and generate more revenue by adopting a transparent security strategy

Introduction

Before SaaS applications became the norm, securing your environment was much more straightforward. Everything was hosted on-prem, providing security teams more control over protecting their businesses. As SaaS became more prevalent, that control was lost. Now, every third-party application that is added to help run the business is a potential entry point for hackers and other bad actors to access your customer data.

So how do companies take that control back? What we're about to propose might sound strange at first but it has been confirmed over and over again through various research studies conducted by Whistic. We've found that the best way to shore up your business against the threat of a potential breach is not to lock everything down and keep everything hidden, but rather to be open and transparent about your security posture.

Jake Bernardes, VP of Security and Compliance at Whistic, says, "A transparent approach and a supply chain built on trust is the only way we can mutually secure and protect our respective assets and data."

We've said it time and again: a company's security is only as strong as its weakest vendor, which is why we suggest taking a collaborative rather than combative approach to vendor assessments. When companies and vendors are transparent about both what their expectations are for a vendor assessment and what their security posture is, everybody wins.

But the end result isn't just a more secure environment for everyone involved. Transparency also leads to faster sales and buying cycles because it shifts everything to the left, meaning security discussions are happening at the very beginning instead of waiting until right before contracts are signed. This ensures employees have the tools they need to run your business and that a vendor's security posture isn't blocking deals from closing. That means more time and resources for infosec teams to focus on more strategic tasks and more money in the pocket of your sales team. If that isn't a win-win scenario, I don't know what is.

The future of security reviews: Zero-Touch Assessments

If we're being honest, vendor assessments aren't fun for anyone involved, especially if your company is using an out-dated, mostly manual, Excel-based solution that forces you to spend hours chasing down vendors or responding to questionnaire requests. Luckily, there's been significant advances in the vendor assessment space in recent years, but there's still a lot of room for improvement.

The future of security reviews are Zero-Touch Assessments. For those unfamiliar with the concept, Zero-Touch Assessments occur when a vendor publishes a security profile publicly (either on their website, or a third-party marketplace or directory), enabling the customer to conduct an assessment without having to chase down information from internal stakeholders and the vendor.

If you think this scenario is a pipe dream, think again. This is the direction infosec and sales teams want to go. Whistic's *2022 State of Vendor Security* found that 94% of companies surveyed would be willing to start a vendor assessment with a Profile, which is a 15% increase from the previous year. On the vendor side, 80% of respondents would be willing to publish security documentation publicly. Finally, 96% of respondents would be more likely to purchase from a vendor that's transparent about its security practices.

The main reasons businesses start publishing their security posture publicly or sharing that information proactively according to the *2022 State of Trust and Transparency* are it shows a commitment to transparency, speeds up sales and buying cycles, and it lets the sales team focus on selling (as opposed to responding to assessment requests).

This process saves time and resources on both sides of the transaction. In the following sections, we'll delve into the impact transparency has on both vendors and their customers and provide some real-world examples of how to make your organization more transparent.

The impact of transparency on sales teams

In the past, security reviews have acted as a huge roadblock for sales teams. They slowed the sales cycle down significantly and, in some cases, caused deals to be lost outright. Our research found that 89% of reps have at least one deal push per quarter because they couldn't respond to a security review in time.

Oftentimes winning or losing *one* deal can be the difference between a sales rep hitting quota or being put on a performance improvement plan. That's why we set out to determine the cost of having an antiquated vendor assessment process in place, which in turn will reinforce our claim that when businesses are more transparent, they will not only save time and resources, but also help sales close deals at a faster rate.

Using data derived from the *2022 State of Vendor Security*, we've calculated time and money that could be saved by publishing and proactively sharing your security documentation with customers. The report found that sales reps are spending 7.4 hours per month answering security reviews instead of selling. Based on a conservative estimate of an $80,000 annual salary, this costs the company $3,652 annually per sales rep, and that's not counting the potential sales they could be making if they could stay focused on that task.

Average Rep Salary	$80,000
7.4 Hrs/month x 12	89
Cost per hour	$41.03
Total Annual Cost	$3,652
Annual Saving w/Whistic per rep	**$2,556** **(@70% acceptance rate)**

As we mentioned, security reviews often cause reps to have deals pushed or lost altogether. If you could save just one deal per rep, what could that mean to your company? A small SaaS startup with an average deal size of $20,000 and a team of 10 reps could translate into $560,000 annually. Even if you were more conservative in your approach and cut that in half, that would still be more than a quarter of a million dollars in the bank. And the impact it could have on the bottom line for individual sales reps hitting quota will ensure team morale remains high.

Avg. ACV	$20,000
Number of reps	10 x 70% = 7
Total ACV lost	-$140,000
Total lost annual revenue to unlock with Whistic	**$560,000**

The impact of transparency on infosec teams

Right or wrong, infosec teams have been viewed as a blocker to business. Whether you're an employee wanting to implement a new solution to help you do your job better or you're a sales rep trying to push a deal through, before you could get what you wanted a security review had to be completed.

Not to belabor the point, but in the past vendor assessments were time-consuming and labor-intensive for both buyers and sellers. However, as we've outlined above, when transparency and vendor/customer collaboration become a priority, buying and selling cycles are accelerated, which makes everyone involved happy.

The *2022 State of Vendor Security* found that vendors are responding to 23 assessment requests per month and that each response takes 3.5 hours to complete, or 80 hours per month. Assuming an annual salary of $125,000 for a security analyst, which comes to $64.10/hour, it costs a business $5,128/month for that analyst to respond to assessments.

Much of those costs can be eliminated with transparent and proactive vendor security practices. When you build a robust security profile, you no longer need to respond to one-off requests. You provide the information to your customer at the outset of the relationship, or even better, they conduct a Zero-Touch Assessment based on security information you've published, and there's no additional work required on your part.

Based on a very conservative profile acceptance rate of 70% (many Whistic customers have a greater than 90% acceptance rate), the number of questionnaires that need responses based on the scenario above would be reduced from 23 to 7 per month and cost $1,538/month, which is a savings of $3,590/month. Annualized that results in a savings of $43,080 or ⅓ a security headcount. Creating more time for analysts to

SquadCast saves 12.5 hours on average per assessment request by publishing its Whistic Profile to its website which enables prospective customers to conduct Zero-Touch Assessments and empowering its sales team to proactively share its Profile at the outset of sales cycles.

SquadCast

focus on other security-related tasks is key, especially in this job market where the demand for their skills is high, so it's harder and harder to find and hire them.

There's also a number of areas where infosec teams on the buying side can save time assessing vendors. Based on results from the *State of Vendor Security*, the average business assesses 13 vendors/month. Each assessment takes approximately 3 hours to complete, resulting in a cost of $2,499/month or nearly $30,000 annually. When you implement a tool like Whistic, that automates much of the processes, including vendor intake, assigning inherent risk, vendor follow up to name a few, it can cut assessment time by 50%, which results in a $15,000 savings annually. And if the vendor being assessed published their security documentation publicly, that savings would be even greater.

Average Response Time Savings with Whistic

Average # of monthly responses	$80,000
Average response time per response	3.5 hours
Total response hours per month	80 hours
Conservative profile acceptance rate	70%
Response hours spent w/ Profile	24 hrs/per month
Wage for 1 security head ($125K/yr)	$64.10/hr
Response cost w/o Whistic Profile	$5,128/per head
Response cost w/ Whistic Profile	$1,538/per head
Monthly savings w/ Whistic Profile	$3,590/per head
Annual savings w/Whistic Profile	**$43,080/per head**

50% Decrease in time spent assessing vendors **using Whistic Assess**

83% Decrease in time spent assessing vendors **using Whistic Assess *and* Profile**

How to incorporate transparency into your vendor security strategy

To help you increase the levels of transparency at your company, we've compiled a list of recommendations and best practices that can easily be implemented and will increase trust with your customers and prospects.

Find partners willing to collaborate

The key to creating an effective, transparent vendor security practice is finding good partners who are willing to collaborate. Jerry Bryant, Senior Director of Security Communication, Product Assurance and Security (IPAS) at Intel, puts it this way, "Security is a collective, shared responsibility, and it takes cooperation among vendors, system providers and end users to implement mitigations quickly and effectively. But without a commitment to security transparency—particularly from technology industry leaders and vendors—building public trust and security assurance simply isn't possible."

Public trust in companies is eroding with each passing security breach, so it's going to take a commitment from everyone to be open with one another about security in order to both win back trust. You should seek out vendors and customers who are open to creating partnerships built on a secure foundation. This will be more difficult if you work in traditional industries like finance and healthcare that are slower to adopt new technologies and may still try and force complex Excel docs down their supply chain. Just because you're willing to change quickly, doesn't mean that they are, but if they refuse to change, they will continue to be more vulnerable to breaches.

Participate in Industry Consortiums

Join groups like NIST, CSA, and Security First Initiative to help define common best practices for increasing transparency, reducing risks, and limiting the impact of third party security incidents. When Whistic formed the Security First Initiative in May of 2022, we did it with the goal of making transparency around security practices the rule not the expectation, and top technology companies like Okta, Airbnb, Zendesk, Asana, Atlassian, Snap, Notion, and Drata saw the vision.

In fact, Drata's CEO Adam Markowitz said when they joined, "At Drata, we are staunchly focused on easing the path to continuous compliance and guiding our customers with transparency. Joining the Security First Initiative furthers our ongoing commitment to building trust on the internet, starting with our own security posture."

When a company's security is only as strong as its weakest vendor, it makes it even more imperative to partner and collaborate with security-minded vendors.

Build an informative security page

Next, you should build an informative security page on your website if you haven't already. It should include links to your privacy policy, instructions for accessing all of your security documentation, including responses to standard questionnaires along with any certifications and audits you may have completed as well as contact information for your security team. Finally, provide an overview of your security program, including information on what encryption you use, your incident response plan, and information related to your disaster recovery/business continuity plan.

Make vulnerability disclosure easy

Earlier this year, Whistic reviewed the security pages for Cloud 100 companies to identify trends as well as areas for improvement as it relates to transparency and vendor security. At the time, only two percent of pages included vulnerability disclosure forms, and just nine percent had bug bounty programs. Adding these two items to your security page is easy to do and a good way to increase trust and show that you are open to collaboration with your customers.

Be open to validation

While the goal of transparency is to build trust with your customers, don't be offended if your customers feel the need to validate the documentation you provide. It doesn't mean they don't trust you. It just means that they're doing their due diligence to ensure their customer data is protected from third-party vulnerabilities that may exist.

In fact, recent research by Whistic and RiskRecon found that more than half of businesses trust the information provided by their vendor. While 62% use a third-party tool to validate questionnaire responses and other security documentation. The easiest way to validate questionnaires is by integrating your security profile solution directly with third-parties who can validate those controls almost immediately.

Using Whistic to improve transparency

One of the primary goals of Whistic is to make it easier for buyers and sellers to connect and collaborate on vendor security reviews. A big part of that is creating a network of like-minded companies that value and promote transparency. There are a number of features and functionality that streamline the vendor assessment process and make it easy for vendors to be transparent with their customers and for customers to help foster a relationship of transparency with their vendors.

The power of the network

Whistic harnesses the power of its Vendor Security Network to connect buyers with the security information of more than 50,000 vendors, enabling them to assess vendors on their timetable before even engaging with them in a sales cycle. Publishing security documentation, including completed questionnaires, certifications, and audits, to the Vendor Security Network is a good first step for SaaS businesses to build trust with customers.

Whistic is showing its commitment to transparency and growing the network by offering any company the opportunity to share and publish their security documentation to the network for free using a Basic Profile.

Get your own Whistic Basic Profile for free

- Eliminate time-consuming questionnaire requests
- Access Whistic's extensive library of standard questionnaires
- Share your Basic Profile with customers up to three times per month
- Publish your Basic Profile to the Whistic Network

Get started at **basic-profile.whistic.com**

Previously Hollard Insurance needed two full time employees just to manage security reviews. Since implementing Whistic Assess, the company has been able to refocus those employees to other tasks, without needing to hire additional headcount to manage the review process. One reason Hollard was able to reduce the amount of time it takes to assess vendors was the ability to conduct Zero-Touch Assessments the Whistic Trust Catalog provides.

Hollard.

Proactively share your Whistic Profile

After you've published your Whistic Profile to the Vendor Security Network, the next step is to proactively share it with customers and prospects at the outset of the customer relationship. Whistic makes this really easy to do for your salespeople with our Salesforce integration, which enables you to share your Profile directly from Salesforce. Doing this will save your InfoSec team countless hours spent responding to one-off questionnaire requests while also building trust with your customers because of how open you are with them.

Whistic Assess significantly reduces the amount of time it takes to assess and onboard vendors. One of the leading providers of business continuity as a service reduced the amount of time it takes to conduct a security review by 91% after implementing Assess.

Whistic Profile helps businesses eliminate one-off questionnaire requests and has a higher acceptance rate than you think. The infosec team at Matterport, the leading provider of 3D printing technology, notes that approximately 95% of its Profile shares are accepted by customers, which has virtually eliminated requests for the team to complete custom questionnaire requests.

Matterport™

Make transparency the expectation for your vendors

On the buying side, you need to hold your vendors' feet to the fire and demand that they share their security posture with you in a timely manner. With Whistic Assess, we've automated many of the manual processes that used to take up hours of your time, like vendor intake and assigning inherent risk, while providing you with a library of standard questionnaires and frameworks you can request your vendors complete.

About Whistic

For many businesses, security assessments are a double edged sword. They have to both evaluate vendors and respond to vendor assessments. With so many assessments coming in and out, it can be hard to keep a handle on everything. To streamline the process for both the buying and selling side of the business, you should consider implementing a solution that can handle both sides of the assessment.

That's where Whistic comes in. Whistic is the network for assessing, publishing, and sharing vendor security information. With Whistic you can:

- Automate key activities in the vendor assessment process.
- Communicate the information your customers need, when they need it.
- Empower customer-facing teams to be transparent about your security posture.

Visit **whistic.com** to learn more or to request a demo, or visit **basic-profile.whistic.com** to try it for free.

whistic