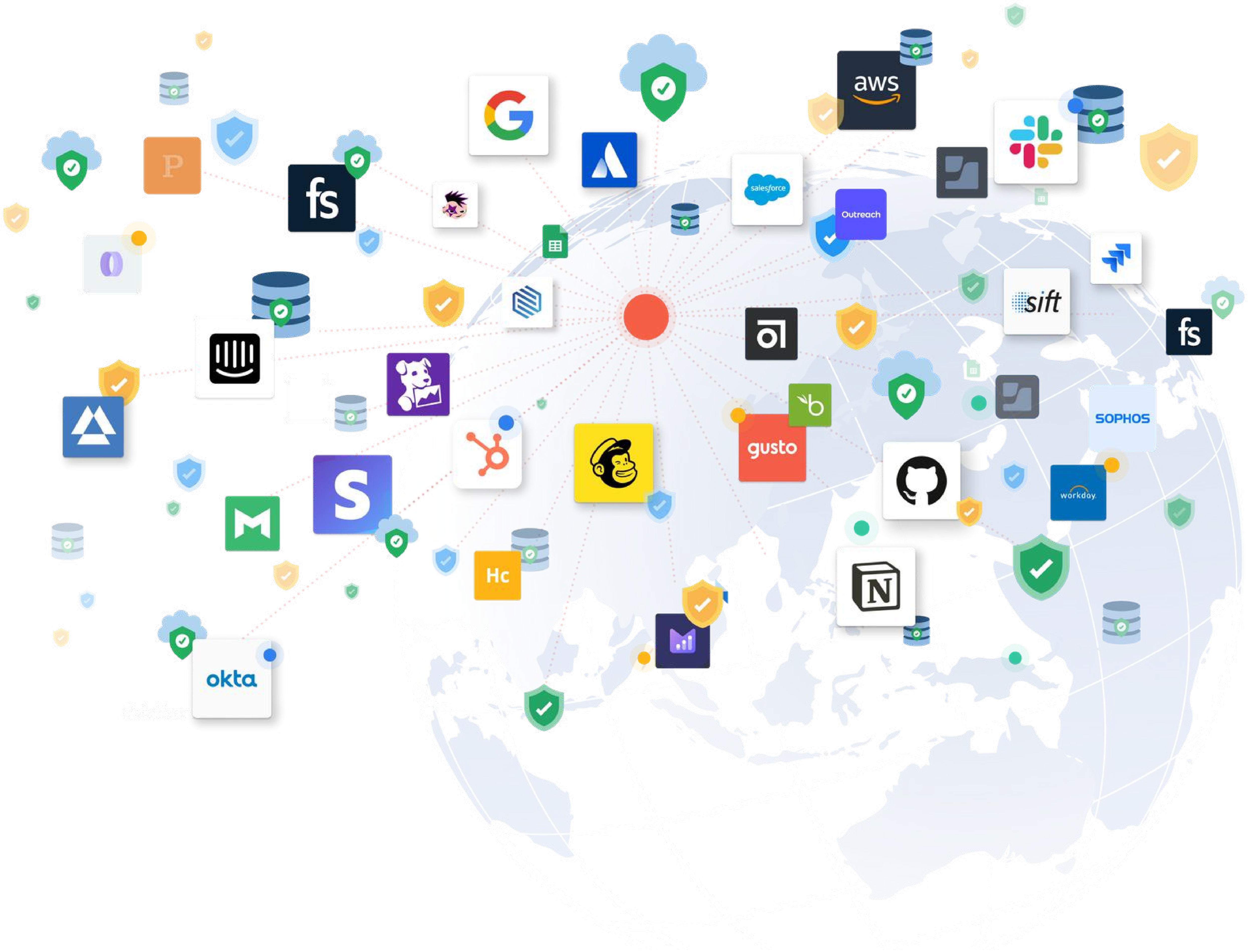
Conveyor

conveyorhq.com

Building Trust on the Internet

Turn your security posture into a competitive advantage



Building trust with customers is more important (and complicated) than ever before

“Oh no. You’ve got ***another*** prospect in the pipeline? Dang it!”

This is not a phrase you’d expect to hear in the B2B software world, is it? For cloud vendors and growing SaaS companies, growing customer adoption at an exponential rate is critical to long-term success. Yet, if you're the person who's stuck answering all those custom security questionnaires from prospective customers, asking to see SOC 2 reports, pen tests, and information about data handling, you might not be so excited every time your sales team comes to you with another "urgent request" to respond to a security review. But in today's world, where more and more business is conducted in the cloud, quickly and proactively building trust is more important than ever before.

SaaS growth isn’t slowing down anytime soon

The overall spend per company on software-as-a-service products is up by 50% compared to two years ago. The average company uses 137 unique SaaS applications on average.

Why is this? Well, in order to move quickly, organizations can’t build every back office, sales, marketing, and product experience and simultaneously build a highly differentiated product. To stay agile, competitive, and cost-effective, companies have become increasingly reliant on external tools to help manage their business and realize their goals. Do you need analysis on the customer journey? There's a SaaS product to do that! Do you need to automate emails to go out to customers with usage tips? There's a platform for that! Do you want to talk to your customers and prospects while they're on the website? Guess what? There's a SaaS tool for that! You see our point.

More than 50% of companies put vendors through a security review

When sharing sensitive data, the cost of a databreach can be more than just financial. Companies are acutely aware of the risk they take on when dealing with third party vendors, so they are doing due diligence with more and more vendors.

While buying solutions instead of building them can be a quick fix to fill a business need, it also opens the door to new risks. Simply picking a vendor to fill the gap is the easy part. Sorting through all of the available options, evaluating the capability and security of each vendor, and finding a vendor that is within your organization's risk tolerances is difficult and time-consuming. As businesses share sensitive data and become more interconnected, the importance of establishing trust between customers and vendors grows. Whether you are a vendor trying to prove your trustworthiness in order to land and retain customers, or you're a client looking to prove that the vendor you're evaluating is as low-risk as possible, trust is more important than ever before.

What is trust on the internet?

Here at Conveyor, our purpose is to build trust on the internet. But what exactly do we mean when we assert that we want to build trust on the internet? While we aren't in control of the internet's technical implementation, we see untapped potential in the way businesses connect and communicate in the pursuit of building trustworthy relationships.

We are sharing information at an ever-increasing rate and there is no shortage of apps to connect two parties. And there are implications for both parties: the vendor and the customer. For the purposes of this post, we'll focus on the plight of the vendor who is trying to build trust with their customer (if you're a customer who wants to learn more about how to effectively manage your vendors and assess trustworthiness, check out this article which gives a great approach to "leveling up" vendor management).

There are some formidable challenges for companies when building trust with their customers:

- Handling up to 100 security questionnaires per month
- Answering non-standardized (oftentimes vague) questions about security
- Bargaining with customers who want more than the security documents (such as SOC 2 and pen test summaries) that you worked hard to achieve
- Taking 6-10 hours (sometimes more) just to complete one security questionnaire
- Coordinating multiple departments that are involved in responding to security questionnaires
- Creating a secure and scalable way to share evidence of trustworthiness with customers in a centralized location

For most companies this process is ad hoc, inconsistent, and time consuming. Add to that the fact that the security questionnaire process usually doesn't happen until late in the sales cycle — when time is of the essence. It leads to a pressure-cooker situation where the go-to-market teams are putting significant pressure on the security team to complete the questionnaires, and the security team needs to shift focus from their work to address the urgency.

Imagine a place where all of this information is pre-populated and can be sent to prospective customers (securely) without dealing with wasted time emailing back and forth. That type of information sharing helps organizations build trust with their customers and prospective customers, and it's how we see the future of doing business on the internet. (If you want to see how you can start sharing security docs with your customers, check out our free Rooms product).

More and more, organizations are spending hundreds of hours (and tens-of-thousands of dollars) pursuing compliance certifications like SOC 2, ISO 27001, PCI, and others in order to validate that their business operates in a trustworthy manner. But simply having those compliance certifications is not always enough to satisfy the security inquiries of the customer (or prospect) and close the deal. Questionnaire frameworks like CAIQ, SIG, and SIG lite were developed in an attempt to standardize the security questionnaire process between clients and vendors. Yet even with the existence of those templates, custom questionnaires persist. And depending on the types of data that will be shared and the access to critical systems, those custom questionnaires can be several hundred questions long.

In this guide, we'll discuss what are some of the critical activities that organizations can take (in addition to achieving compliance certifications) to build trust with their customers and prospects. Then we'll present ideas for how to share security posture early in the sales process to make more efficient use of your internal resources, reduce delays in the sales cycle, and turn your security posture into a competitive advantage.

Trust Building Pursuits

As a vendor, the success of your business is directly tied to the trust and confidence your customers have in your product. Flashy marketing and gimmicky features may make quick sales, but you want to build lasting relationships, not transient ones. Increasing customer retention by just 5% can increase profits anywhere from 25-95%. And thus, it is understandable why the sales organization so urgently needs security questionnaires answered as quickly as possible.

While some may be quick to judge data security activities in the sales cycle as non-essential, there is clear data that customers do prioritize trust when choosing services and products. According to a 2020 report by Prevalent, over 50% of organizations are conducting third-party risk assessments, highlighting how important vendor risk management is to them. Some of this is driven by regulatory requirements (SOC 2 and PCI DSS, for example, have requirements around vendor review), and some of it is due to being burned by exposure to cyber risk in the past (SolarWinds, anyone?)

If you're a company who's on the receiving end of these custom security questionnaires, making it easy to share your security posture is more important than ever before. In addition to adding potential value to your sales process, the work you do to become trustworthy can directly benefit your organization's day-to-day operations. The financial and reputational impact from data breaches is much more impactful than any resources spent on internal compliance activities. If you are breached, potential impacts include:

- Loss of business to competition
- Damaged reputation and negative press
- Disruption to operations
- Increased insurance premiums
- Inability to attract and retain talent

The list above is not exhaustive, but it paints a clear picture that actions that build trust benefit not only your customers but could potentially protect your business from significant losses.

As a vendor, what are some activities you can pursue today if you want to improve your ability to build trust with customers?

Compliance certifications

The most common way companies prove they are trustworthy from a data security perspective is by achieving compliance certifications. Some businesses have legal or regulatory obligations which often require good data security practices but don't provide any certification to prove to customers that they are being met (ex: CCPA, GDPR, and HIPAA). Many more businesses can benefit by undergoing an assessment to certify they are meeting compliance framework requirements and receive a report proving their security posture.

For example, the Department of Health and Human Services does not endorse any HIPAA certification, and there is no standardized certification and accreditation process. While some companies claim to be HIPAA certified, there is no such designation. Other frameworks such as PCI DSS require that merchants and service providers attest to their compliance through assessment by designated external entities known as Qualified Security Assessor Companies (QSACs), or self-assessment, depending on the organization's size and transaction volume.

In addition to simply understanding whether or not you need to be assessed and certified against a law, framework, or standard, you must also understand the details of the assessment, certification, and reporting process:

- Who can perform the assessment?
- Is the assessment point in time or over a period of time?
- What are the reporting requirements?
- Once I receive my assessment report from my auditor, do I need to communicate it to a governing body?
- How long is the certification valid?

Regardless of what you are certifying against, the process requires work. The above questions can help ensure your efforts to comply with a given law, framework, or standard are rightly recognized and that you can successfully maintain that compliance for as long as it is needed.

Sharing security documents

You've spent time implementing a security program, complete with policies, procedures, controls and you've even gathered evidence to show that the program is healthy and functioning. Now what? We say sharing is caring! When it comes to trust, security platitudes are cheap, sharing the tangible evidence that your organization is up to the task of supporting a customer's mission is as good as gold. Putting the control in your customer's hands and not getting in their way with arbitrary gatekeeping allows them to move quickly and you to focus on maintaining your program.

When it comes to sharing trust building content, you can aim for the status quo, or you can think outside of the box. Talk to your sales team and review customer contracts to get an understanding of customer requirements and what can help accelerate the pipeline. Your program is not your competitors, so why does the content you provide look indistinguishable from theirs? Policies, procedures, ISO 27001 Certificate, SOC 2 Report — these documents say you meet certain expectations but don't highlight what your organization does to exceed them. Find opportunities to stand out. Some considerations for atypical evidence to share include:

- **Penetration Test Report** - Sharing the content of a recent Penetration Test shows transparency and demonstrates the true effectiveness of your program's controls against a trained threat actor. While we don't recommend presenting this as a document that you share with every potential customer, for high-priority partnerships, this level of openness could help solidify a valuable partnership. We also recommend that you share the version of the penetration test where exploitable vulnerabilities were remediated and re-tested. This will limit risks to your organization that there is not potentially a document out there with live vulnerabilities and step-by-step details on how an attacker exploited them.
- **GRC Evidence** - If you have a GRC solution that collects evidence and assesses it against desired configuration states, this information provides valuable information on the health of your controls over time. We're not saying to share the raw data of the payloads; those could contain sensitive information about the environment. However, if your implementations track statuses of key security controls such as MFA enabled, adequate password and lockout policies, or even change management controls such as reviews and approvals of code and infrastructure changes. This can show your potential customer that not only are you aware of best practices, you are committed to effectively implementing them.
- Issues and Events - There are unforeseen circumstances and impediments that all businesses face. Recently, there has been a shift away from the knee-jerk reaction to vilify these organizations when issues occur but rather appreciation when the issues and resolutions are openly communicated. If your organization uses a status page as a communication tool for incident response activities, make customers aware of it. Demonstrating a commitment to transparency and openness will reassure customers that your organization will not compound issues by delaying action or denying impacts.

- **Subprocessors** - If you have to comply with GDPR, you are already familiar with the process of communicating your list of current sub-processors. As more businesses become entangled through vendor relationships, a breach at one vendor can cascade, affecting their customers, and their customers' customers. These fourth party connections have traditionally been viewed as going too far down the rabbit hole when scoping vendor risk assessments. However, recent incidents such as the SolarWinds Orion breach show that incidents of vendors do not stay localized for long.
- **Social Proof** - With the sheer number of vendor options, sometimes sifting through the search options can be overwhelming. Sharing real customer stories can go a long way in building trust. Being the first to test the waters can be nerve-racking and even detrimental, however, you can feel much more confident when peers in your industry are telling you "jump in, the water is fine!"

Receiving a security questionnaire from a potential customer often comes late in the sales cycle. By sharing some (or all) of the above earlier in the sales conversation, you can help avoid delays in the sales cycle, and eliminate a mad rush at the end of quarter when the security team often gets hit with dozens (or more) independent questionnaires. For more information on the ways in which security documentation can be shared securely with individuals outside your organization, check out this post.

Trust Pitfalls to Avoid

Falling short in establishing trust can cause significant business impacts. Additionally, since this process doesn't happen in a vacuum, you need to consider not just the impact to yourself but the impact to your partners, customers and vendors. Here are some common pitfalls to avoid.

A few "don'ts" when creating trust:

- **Lack of Transparency** - Your prospective customer wants to make the most risk informed decision when picking a vendor, and that decision will require some data analysis. Trust isn't built on blind faith and secret keeping. Refusing to provide even the most basic evidence requests will not help you solidify a sale. As a vendor, your job is to make the customer feel at ease about your product or service. If you are finding that customer data requests are becoming too cumbersome to handle in both volume and uniqueness, consider implementing a customer self service portal and sharing your documents up front. This can put the prospective customer at ease and reduce the need for more back-and-forth.
- **Misleading Marketing** - In today's market where there are literally thousands of SaaS products, there is so much competition that simply stating your product can be trusted is not enough. You need to prove it. With the rise of compliance and certification frameworks, companies who rack up the most badges get to cut to the front of the line for potential customer evaluation. While compliance certifications may lead to better deals, they are neither quick nor inexpensive to achieve. Some companies may turn to deceptive tactics to reap the benefits of compliance without actually making the investment. Never use deceptive tactics like using compliance badges on your site or presenting customers with non-official attestations or certificates if you did not actually earn them.
- **No justification for "No"** - When you receive requests for compliance evidence or are answering questionnaires and you have to answer "no" to a request, not providing a justification can harm your chances at solidifying a new partnership. You can't be expected to meet 100% of all customers' requirements, but you should be prepared to have well-articulated, thoughtful responses for all requests. Suppose you receive a request that requires you to have a Dynamic Application Security Testing (DAST) tool in place. If you don't, don't fret, all may not be lost. Do you perform static code analysis? Do you contract with a third party to conduct periodic application penetration tests? If so, explain these controls! There is no single recipe for achieving a secure or risk mitigated state and your customer should welcome these kinds of discussions. Always remember that trust is collaborative. We can't solve vendor trust problems if we only look at a single side of the equation.

Now what?

We’re in the business of providing solutions, not just providing commentary on issues. Take some time to see how Conveyor can help build more trust with your customers, move the security conversation earlier in the sales cycle, and make customers feel empowered in their ability to access the information they seek.

If you have any questions, you can contact us at hello@conveyorhq.com.