SOC 2 Type II Compliant Live Chat Software: What You Need to Know

You want to provide the best service to your customers, so you offer live chat support and let them get answers to their questions with a few clicks of a button.

But even in a world of instant satisfaction, it's important to take a moment and verify your live chat software provider has taken the necessary measurements to keep your customers' sensitive information, which they trust you with during chats, safe.

If your provider has a SOC 2 Type II certificate, you can sleep well at night.

What is SOC 2 Type II Compliant Live Chat Software?

The American Institute of Certified Public Accountants (AICPA), who established the SOC 2 protocol, defines it as a "report on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy."

In other words, to be SOC 2 certified, live chat software providers need to get a professional audit of their documentation and control framework – including cybersecurity policies, technical tools, and how they control access to their resources (among other, how they control access to *your* customers' sensitive information).

In this context, a service organization isn't only a company that provides traditional services, like consulting. A SaaS company is considered a service organization too. It just provides software as a service. Most companies get a live chat software in a SaaS model, meaning their live chat software providers are eligible for SOC 2 certification.

SOC 2 Type I vs. SOC 2 Type II: What's the Difference for Your Live Chat Software?

Like other service organizations, live chat software providers can be certified in two types of the SOC 2 protocol. Each type results in a different audit and, therefore, in a different type of report.

SOC 2 Type I Means Your Live Chat Software Provider Did a Good Job at the Specific Time of Auditing

A SOC 2 Type I audit looks at how your live chat software provider handles cybersecurity at one specific point in time.

There is no assurance it handles it well over a period of time – just at that one specific point it was audited. It might be doing great, and it might have had it employees working overtime in the last minute, just to pass the audit.

SOC 2 Type II Means Your Live Chat Software Provider Has Been Continuously, Efficiently Cybersecure for a While

If your live chat software provider has a SOC 2 Type II certificate, it means it has been audited and certified for doing a good job with cybersecurity for at least six consecutive months.

Generally, the entire process for Type II, including preparation, can take a year, versus only 3 months for Type I.

Type II is a much deeper, more thorough auditing procedure. It signifies the provider has put some processes in place to be able to deliver high quality cybersecurity over a long period of time. Not only that, but the audit ensures the implemented policies, processes and technologies have actually proven effective over time.

Why Your Company Needs SOC 2 Type II Compliant Live Chat

Not every company needs its live chat to be SOC 2 Type II compliant.

If your live chat reps don't handle sensitive information – for example, if you only answer general product questions, provide opening hour information, or give non-personalized advice – you might not need to worry about it.

But if you're looking for a live chat software for a bank, a healthcare organization or an ecommerce company whose live chat reps answer questions about specific customers' accounts, SOC 2 Type II becomes critical.

In fact, anyone who handles passwords, credit card information or other sensitive data needs to care about the security of the information their customers entrust with them and their software providers. That's true even if your company specializes in developing gaming apps.

SOC 2 Type II doesn't guarantee there will no breaches, but it does mean your live chat service provider has gone above and beyond to secure you and your customers, including:

Keep Your Live Chat Data Safe

Many providers take partial steps to keep your data safe. For example, many providers are PCI DSS compliant, which means they erase credit card numbers from live chat transcripts and data.

But PCI DSS is only invoked when someone is trying to pay. If a customer authenticates personal information via chat, so you'll tell her how much money she has in her savings account right now, it's still kept in the chat transcripts, and it can be stolen.

SOC 2 Type II audits ensure the data is as safe as it can be. It ensures that it's very hard to crawl and steal your transcripts.

Ensure Hackers Can't Get into Your System Through Your Live Chat Software Provider

Many live chat software providers integrate with their partners' accounts through single sign on. Hackers that hack your live chat software provider can ride prebuilt API pathways, and use your provider to open the door to your bank or hospital's system.

SOC 2 Type II audits check how your provider has prepared to prevent it. If your provider has passed the audit and received certification, it's as safe to partner with it as it can be.

And if, despite taking all the possible precautions, a breach happened?

Detect Anomalies and Block Cyberattacks on Time

A software provider that's been SOC 2 Type II certified usually has systems to monitor your live chat operations on a regular basis, so it can detect when things look off. For example, if you usually get 100 chats a day, and suddenly that skyrockets to 10,000 a day, your provider's system will alert it.

Then, the provider's IT team can explore what happened, check with you if you know about it (maybe you've got a campaign going on or you're doing some testing), or whether it's a cyberattack that needs to be stopped.

Instantly Diagnose the Problem

These software providers usually go even deeper. They have systems that not only identify a problem – but diagnose what the problem actually is.

This way, if data gets compromised, they don't need to figure out from scratch why it's happening, which could take a while. They get an immediate diagnosis, so they can move much faster toward taking action, to minimize the damage.

Prevent it from Happening Again (Based on Actionable Data)

Similarly, certified providers are able to provide actionable forensics. They're able to know when an attack happened and why, how much data was compromised, and how to fix it for the future, to prevent it from happening again.

So Why Don't All Contact Center Software Providers Offer SOC 2 Type II Compliant Live Chat?

In two words, it's hard.

First, there's a rigorous auditing process, which requires a ton of work from your team, including in depth reviews and continuous requests for more and more information, and more and more meetings. Here at our company, the entire process took a year, including in-office audits in both our Vancouver and China branches.

In addition, it's expensive.

And paying for the audit itself is not the biggest expense.

Making sure your data centers are robust enough, hosting your servers at centers that also went through this certification, and making sure your IT experts are available 24/7 – these are some of the bigger expenses.

Wait, Aren't All Contact Center Software Providers Obligated to Offer SOC 2 Type II Compliant Live Chat?

The surprising answer is no.

Getting a SOC 2 Type II compliance certificate is a totally voluntary process.

Live chat software providers have other obligatory regulations to meet, like HIPPA, especially if they partner with highly regulated industries. Each compliance procedure is expensive and time consuming.

For some companies, it might not be a priority to go through voluntary compliance processes on top of that, or they might not have the resources (remember, it took us a year and cost a ton – it's not easy).

But you can't afford to comprise your company and customers' most sensitive data.

How to Know if a Contact Center Software Provider Really Did Everything Right to Offer SOC 2 Type II Compliant Live Chat

No live chat software provider will share its SOC 2 Type II certification report publicly, because it's unsafe. The report goes into detail about everything the provider does to keep your sensitive information safe, and no one wants this information reaching hackers' hands.

However, providers will usually share these reports in private with verified prospective partners and clients. To request our report, please contact us here [link to relevant page/form/email].

Together, we can create a world of better service that customers can actually trust.