BetterCloud

The IT Handbook to Choosing the Right SaaS App

MEET THE AUTHOR

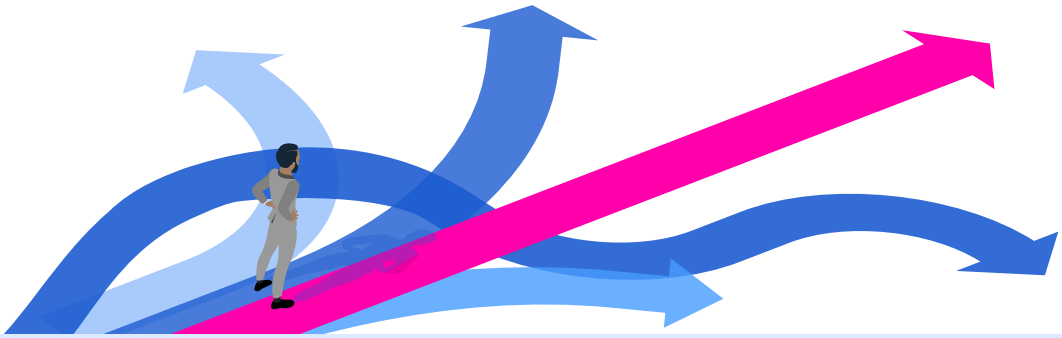
Rose Layton

Rose is a strategic technology partner at Strada Education Network, which is just a fancy way of saying that she does IT strategy and SaaS administration. Originally intending to become a teacher, she leverages that background, along with her nine years of experience in technical support roles, to help build positive relationships between the IT team and other business units, improve IT processes, and work toward a world-class employee experience. Rose greatly enjoys trying and playing with new technology, and the explosion of SaaS apps has given her an outlet to do exactly that. She believes strongly in the power of technology as a force for good, working smarter instead of harder, and getting enough sleep.

INTRODUCTION

Whether you're in a SaaS-powered workplace or just dipping your toes into cloud software as you shift to a remote workforce, one thing is immediately clear: There are so many options out there.

Sometimes, choosing a new SaaS tool means combing through lists of dozens (dozens!) of similar apps, and it can be hard to tell which is the right one for the job. Some tools are called "best in breed"—meaning that they are generally ranked at the top of their market segment. Some obvious examples of best-in-breed solutions are Slack for chat and Zoom for video conferencing. Tools like these offer a positive user experience, superior reliability, and a clear forward-thinking vision about how software can make our workplaces more seamless and productive.



As an IT admin, however, there's a lot more to consider than just "Does this get the job done?" when evaluating a new or replacement SaaS tool.

Today's IT organizations have to deal with an incredible number of applications to administer and secure, on top of our more traditional tasks like supporting users, managing networks, and keeping the business running. And yet, IT admins are still very much needed to help evaluate SaaS applications before purchase. So how do we do this? And more importantly, how do we make this a sustainable, scalable process?

Over the last year, I would estimate that I have formally and informally evaluated about 100 SaaS applications, including cloud phone systems, project management tools, antivirus tools, marketing platforms, content management systems, MDM, and SaaS management tools. Sometimes, I'll evaluate more than 10 apps for a single category! And yet, this is only a small fraction of my overall duties, and definitely only a tiny portion of IT's overall responsibilities. So let's talk about how we manage it.

STAGES OF EVALUATION

Who's out there?

(Googling it, 101)

When any employee or business unit identifies a need for new software (including IT), the first thing I do is get a look at the space. This means using good old-fashioned Google, with specific search terms related to the task that we are trying to accomplish.

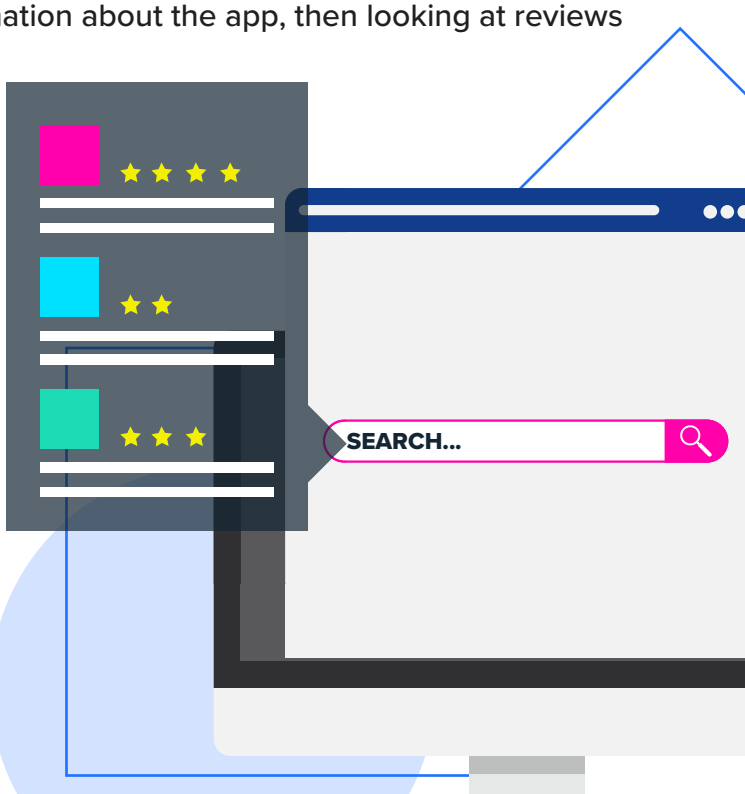
Be sure to include things like "marketing" if you're looking for a CMS geared toward marketing copy, for example. If you have the name of a potential tool already, use sites like G2 Crowd or TrustRadius to find alternatives—but make sure to look in more than one place! The products shown in Gartner's Magic Quadrant may be completely different from the products shown on Product Hunt, for example.

Feel free to crowdsource this part! Some of my most interesting evaluations and eventual purchases came from my teammates, or from my professional network in online IT communities like BetterIT, tabGeeks, and MacAdmins.

Let's have a look...

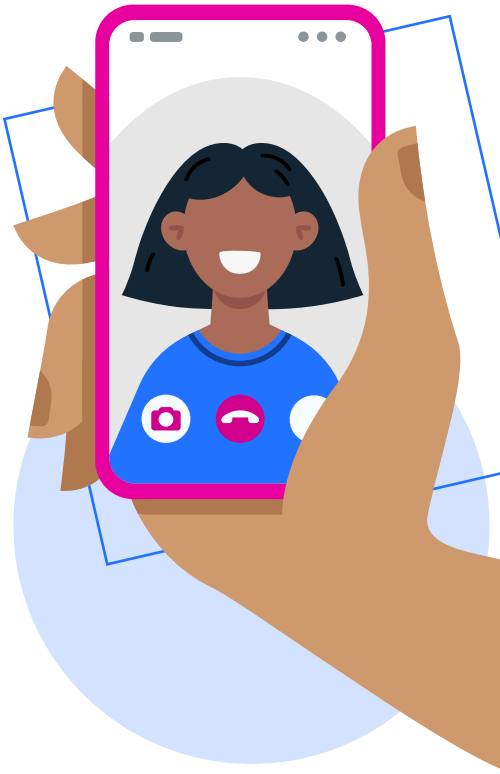
(Initial evaluation)

After you have some names, the first step is the initial lookover. This is where we're trying to decide if the app is even in the right ballpark—if we should cross them off the list now or dive in more. The first step is looking at the website for information about the app, then looking at reviews to see what customers have liked and disliked about it. (This is also why I try to leave detailed reviews on these sites when I can!)



If you are a G Suite shop, and everything on the product website is about Office 365, then you might just want to cross it off your list before going further. Likewise, if your organization has very strong single-sign on (SSO) adoption, and you don't see SSO listed in the features, that would be a red flag in the early stages.

That's not to say that you can't move forward with the evaluation, if you want to! But if you have to look at 12 SaaS products, you are likely to find a winner without having to waste time talking to salespeople and sitting through demos, only to find out that they don't meet one of your core requirements.



Yes, you probably have to talk to that salesperson

(Demo and full evaluation)

Hopefully after the initial pass, you've been able to cross some apps off your list, and you have a few that look promising or that you're excited to learn more about. (Am I the only person who gets excited about using new software? Yes?) This is where you take the next step—yes, you're probably going to have to talk to a salesperson to request a demo.

All jokes aside, trying to talk to a salesperson about their product can be incredibly enlightening. In one instance, I was asked to "sign off" and purchase an application by a different business unit. A visit to the website looked good, but trying to request a live demo and quote revealed something unbelievable... the company didn't yet sell any of the products that were described on the website! I've encountered other instances where salespeople didn't actually know how the product worked, or would talk up features that didn't actually exist yet—all of these issues are more easily caught by someone who is used to talking to software vendors. As I'll discuss in the next phase of evaluation, I also love to see products that offer free trials or demos without talking to someone. These products are usually well designed, easy to use, and offer strong features that stand on their own (and don't need someone to prop them up or demystify them). After all, that's how SaaS became so popular!

What needs are the stakeholders trying to meet? What do you already have in your organization, and how well are they meeting those needs? What are your security policies? What's your budget?

Unlike in the initial evaluation, this is the stage where you're going to need to understand your organizational or stakeholder requirements.

It's impossible for me to tell you what these are for every evaluation and every organization, but here's a little glimpse of some of my general "checkboxes":

UI/UX

Is it easy to navigate? Are the parts of the software laid out in a way that makes sense, or is the navigation "circular"? (Can the same thing be accessed from multiple places, or do I frequently have to go back out of one thing and into another?)

How responsive is it? How does it look on different sized screens or mobile devices? Do the pages load quickly?

How long will it take to learn to use? If I'm going to be rolling an app out to my entire organization, will my end users pick it up quickly, or will I have to train them?

Does the application have self-service support? Do they have public support pages and documentation? Do they have a chat option within the app if someone wants immediate help?

Does using it remind me of Windows XP/2000? (No seriously, this is a real litmus test that otherwise modern applications sometimes fail.)

Administration

Is there transparent pricing listed on the website? How much does it cost relative to other SaaS tools we use?

Does it support SSO? Is it SAML or OAuth? Do I have to pay more to get SSO?

Is there an API? Does it integrate with other tools in our SaaS stack? On a related note, does it support SCIM provisioning? Do I have to manage access manually?

What kind of analytics does it offer? Are they exportable?

Does it offer multiple admin roles? Does it offer custom roles?

What is the support SLA? Is there an option to buy a premium support package, if we want it? How easy is it to get data in (or out)? If we decide to switch products in the future, will we have to start from scratch?

How reliable is the application? If it's hosted on AWS and some AWS AZs go down, do they have continuity built in?

Is it hybrid or cloud-native? This can be more difficult to assess, but the rise of SaaS has also given rise to hybrid applications—where the product is hosted and managed by the providers, but it's still isolated to individual servers and can require regular maintenance outages.

Security & Privacy

Are there system and admin logs? Can they be exported, manually or automatically?

If they send email on your behalf, is the provider able to provide DKIM/DMARC keys?

Do they have available GDPR/CCPA/other privacy documentation? Do they meet the security requirements for our organization?

Do they have security certifications, such as SOC 2 or ISO 27001?

Do they have a policy about data retention/deletion? If so, what is it?

Let me touch it!

(Final evaluation)

As you can see, there's a lot to consider here, and not all of these questions can be answered in a demo or on calls with a salesperson. If you make it out of the main evaluation process and still have a couple of solid products on your list, the best thing to do is to get into the actual product. By digging in and actually using the software, you get the best sense of how difficult it will be to use and administer. Most SaaS apps these days will start you off with a trial anyway, or allow you to use a live demo on your own. These trials are time intensive, though, so I try not to do more than two or three apps for a single evaluation.

By the way, not every evaluation has a clear "winner"—sometimes you'll end up purchasing something that has a less-modern UI because it meets your feature requirements, security requirements, or budget. Very few of the items I listed above are considered "deal-breakers" in my current organization, and if I move to another organization in the future, I'm likely to encounter an entirely different set of "deal-breakers."

One question you might be asking now is "How do I keep track of all this? Is there some kind of template?" There are some out there. Here's a sample spreadsheet to show what a theoretical evaluation could look like when it involves multiple people providing input. But again, nothing is one-size-fits-all. Personally, I usually use a plain document, with notes for each app under their own heading. When you cross one off your list, just remember to make a note of why you did, so if you ever come back to it, you'll be able to see why it didn't make the cut.

With thousands of SaaS apps out there, selecting the right one for your organization can feel challenging. It's important to remember: There's a lot more to consider than just "Does this app get the job done?" By understanding stakeholder requirements, doing your research, asking the right questions, and digging deeper into the software, you'll set your organization up for success in the long run.

If you have any questions or additional suggestions on evaluating SaaS apps, I'd love to keep the conversation going! You can reach me in the BetterIT Slack community as @rose.

BetterCloud

Bonus Content

6 things you should look for when selecting a secure SaaS vendor

Brought to you by the: BetterCloud MONITOR

As Layton mentioned earlier, when you're evaluating SaaS apps, you need to select vendors with the right security measures in place.

This is especially true if you are giving them access to other SaaS applications that are critical to your organization or process sensitive information. Granting a SaaS vendor permissions is like granting access to an account shared by a group of users instead of just one—it dictates the need for more confidence and trust. After all, without proper security, even the best service rapidly loses value when its carelessness could ultimately result in your organization appearing in the headlines. But how do you know if a SaaS vendor is secure? BetterCloud's Security Compliance Director Mosi Platt shared some key things to look for:

1. The vendor presents certified alignment to an accepted security framework

There are a number of different published frameworks (Trust Service Principles for SOC 2, CSA CCM, ISO 27001, NIST CSF, PCI DSS, CIS Controls) that outline guidelines and best practices to manage security risks. Alignment to a framework serves as the plan, but accountability is what ultimately leads to mature security programs. Third-party certification demonstrates accountability. It proves that a vendor has strong security practices in place—that they do what they say.

What security rules does the SaaS vendor follow? How are they managing those rules? Make sure their rules are based on an internationally recognized and accepted standard for security, such as ISO 27001 or the Trust Service Principles for SOC 2.

While an ISO 27001 certification says you meet specific security requirements, it doesn't say *how* in the way a SOC 2 report does. It's the rigidity of SOC 2 compliance that makes it an important consideration for choosing a SaaS provider.

2. Necessary compliance certifications are in place

Depending on your industry or geographical region, various regulatory bodies have compliance guidelines in place (e.g., PCI or GDPR). Before using their product, you need to make sure that your SaaS vendor complies to avoid putting your organization at risk.

SaaS vendors can certify their compliance by providing a self-assessment or independent audit report. A self-assessment typically indicates a lower level of maturity in the vendor's compliance or even the compliance requirements themselves (e.g., a new standard or regulation). A compliance report from an independent third party will provide you more assurance, but likely at a higher cost for the service.

3. There is a clear dedication to information security

There are key qualities that demonstrate whether or not a SaaS vendor is serious about information security. For instance, having a dedicated security team with defined roles and responsibilities is a clear indicator that an organization is committed to accomplishing its security goals.
It is also important to know that they are taking steps to bring in the right people—employees who pass background checks, who don't pose an insider threat. They need to be vetting and training their people. Ongoing educational campaigns, like simulated phishing attacks, instill a culture of security and help mitigate risks.

Access control is also a vital component to information security, and it cannot be an afterthought. Access control only works when precautions are in place to ensure that the right people have access to the right information when they need it.

Are they using secure passwords to protect their access so that no one else can impersonate them? Do they have a solid termination process that revokes access once people leave? Physical security matters too. Make sure the vendor controls access to any facilities housing your information.

Lastly, understand the vendor's encryption policies. Encryption protects transmission and storage of sensitive information, and is a key component in making sure that you're not disclosing information to people unnecessarily. It ensures that transmitted information can only be read by the sender and the recipient. Likewise, when data is being stored, it ensures that data can only be accessed by authorized individuals who have the keys to decrypt it. Is the vendor encrypting data at rest to protect information, even when it's not in use?

4. The vendor's operational security follows known best practices

Do they have a good process for taking inventory of their assets? "You can't protect what you don't know you have," says Platt. There should be a clear process for asset management and protection needs determination (i.e., what information needs very high protection and what doesn't).

Change management is a key aspect here, especially when making system changes or releasing a new feature. Is the asset inventory updated with changes? Do they develop their product in a way that meets security requirements? How do they build security and privacy into new features?

Does a security design process exist? "For instance, we have an automated code review, so that when an engineer writes new code and they check it into our code repository, it automatically gets scanned for security vulnerabilities," says Platt.

Can they provide backup copies of your information, so that if something happens (such as a ransomware attack), you can always get back to a known good state within a reasonable time frame? Can they provide an audit trail of who's actually using your systems? Audit logs can help you detect fraud and make sure there is no unauthorized behavior.

Finally, when issuing a patch to fix a flaw, a process should exist to identify when they're available, while also making sure those patches are tested to avoid negatively impacting users.

5. They are taking the time to properly vet their partners

Forty-four percent of data breaches are directly attributed to vendors. This should be reason enough to ensure that your SaaS vendor is taking precautions including legal and privacy agreements. What controls and processes do they have in place?

Third-party security reviews can play a key role here. “Anytime somebody at BetterCloud wants to use a new third-party tool that will have access to confidential or restricted information, our security team takes a review of who that third party is to make sure they have the right controls in place,” says Platt.

6. A clear plan is in place for incident management and business continuity

No security program is perfect. However, when an organization has a repeatable process in place, it’s possible to manage those incidents without causing additional problems and making things worse. According to Platt, “Repeatable processes help avoid panic by providing an orderly strategy to make sure that everything gets back to a known good state.”

Business continuity is equally important. Are processes in place to make sure services are available when needed? Or when they’re not available, is there a repeatable process to get things back to where the customers need them to be? This could mean hosting the application in multiple zones and data centers to provide needed redundancy. These business continuity efforts make sure that no matter what happens, it’s possible to get the SaaS offering back to where it needs to be.

FINAL THOUGHTS

Security isn’t a “nice to have.” It’s a necessity.

The decision to embrace security often dictates the health and stability of your organization. As such, you are unnecessarily taking your chances when you go with a vendor who fails to embrace security best practices.

While it may require extra effort to make sure your SaaS vendor is actually doing what they say they do across these key categories, it is critical in order to protect your organization.

About BetterCloud

BetterCloud is the first provider of SaaSOps solutions to manage and secure the digital workplace. Over 2,500 customers in 60+ countries rely on BetterCloud to automate processes and policies across a company's SaaS application portfolio. A pioneer of the SaaSOps movement, the company established the first-ever "SaaS Application Management and Security Framework" via two published books entitled "The IT Leader's Guide to SaaSOps" — Vol. 1: "A Six-Part Framework for Managing Your SaaS Applications" and Vol. 2: "How to Secure Your SaaS Applications." BetterCloud is headquartered in New York City, with offices in San Francisco, CA and Atlanta, GA.

For more information, please visit *www.bettercloud.com*.