Your Guide to Winning New Clients

(and upselling to existing ones)

SaaS Alerts™

STEP 1: GET THE MEETING

If you've ever tried to convince a business owner to take a sales meeting, then you know it's no easy task. The question is, how can you demonstrate enough value in your sales pitch to get that first meeting?

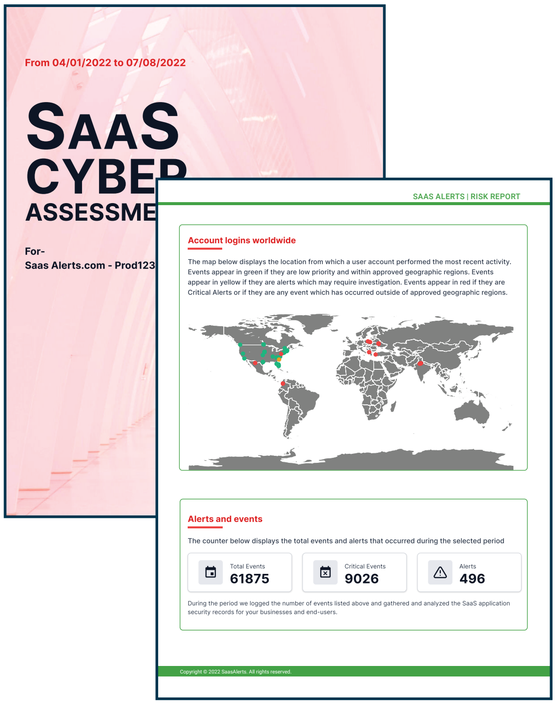
HERE'S THE PITCH:
In just 90 seconds, I'll provide an assessment that will identify brute force attacks, unauthorized logins from different countries, orphaned links from outdated file shares, data exfiltration, a view of confidential files, and more. Make them see that they really don't know what's going on behind the scenes in their most relied upon business applications. Maybe all is secure. Or maybe, like with other clients you've worked with, there's an undetected incident and they're network is at risk.

STEP 2: WOW YOUR PROSPECT

This is where you leverage SaaS Alerts' quick and easy SaaS Cybersecurity Assessment or Risk Report. You can use these reports to identify vulnerabilities in any prospect's SaaS applications, including Microsoft 365, Google Workspace, Salesforce, Dropbox, and Slack.

Many small businesses don't think their business is at risk, but if they have customers, revenue, and a bank account, they are most definitely at risk. And threats can come from both inside and outside the organization. As an MSP with SaaS Alerts in your toolkit, you can identify possible threats in their environment and wow them from the first call.

In your initial meeting, either virtual or in-person, show the prospect a sample report of what you typically detect in your customers' environments and remediate on their behalf. This is as easy as showing the prospect a sample of the Risk Assessment or Cybersecurity Assessment. Conclude by telling them that you can provide the same level of oversight for their SaaS environment. Ask them if they'd like you to run a complimentary assessment on their SaaS applications to see what's lurking behind the scenes.



From 04/01/2022 to 07/08/2022

SAAS CYBER
ASSESSME

For-
Saas Alerts.com - Prod123

SAAS ALERTS | RISK REPORT

Account logins worldwide

The map below displays the location from which a user account performed the most recent activity. Events appear in green if they are low priority and within approved geographic regions. Events appear in yellow if they are alerts which may require investigation. Events appear in red if they are Critical Alerts or if they are any event which has occurred outside of approved geographic regions.

Alerts and events

The counter below displays the total events and alerts that occurred during the selected period

Total Events	Critical Events	Alerts
61875	9026	496

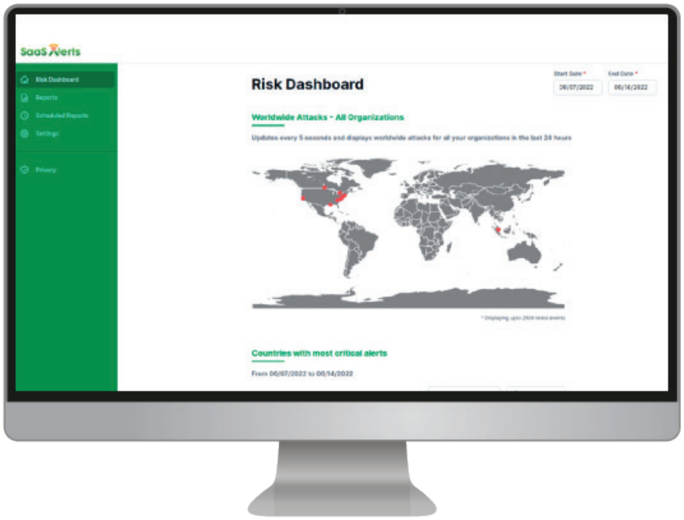
During the period we logged the number of events listed above and gathered and analyzed the SaaS application security records for your businesses and end-users.

Copyright © 2022 SaasAlerts. All rights reserved.

STEP 3: RUN AN ASSESSMENT AND CLOSE THE DEAL

If everything goes according to plan (and we're confident it will), the prospect will agree to an assessment. To proceed, the prospect needs only to enter their SaaS application's global admin credentials into the SaaS Alerts platform to produce a comprehensive SaaS Cybersecurity Assessment Report.

But wait. Why would this prospect simply hand over the metaphorical keys to their castle after a single meeting? This is your opportunity to demonstrate that you have a security-first mindset and build an additional layer of trust from the onset. SaaS Alerts has developed a process for you to do just that.



Risk Dashboard

06/07/2022 06/14/2022

Worldwide Attacks - All Organizations

Updates every 5 seconds and displays worldwide attacks for all your organizations in the last 24 hours

* Displaying upto 2500 latest events

Countries with most critical alerts

From 06/07/2022 to 06/14/2022

Here's the proven process our partners use to gain trust so prospective customers will agree to a SaaS cybersecurity assessment:

1. You've done some of this already, but it's important to educate the prospect on the value the SaaS Cybersecurity Assessment provides. Most companies have very little visibility into the security holes that may exist in their SaaS business applications. Even a single, tiny security hole could damage their security posture. The smallest of blips could lead to a full-blown attack, putting their entire business at risk.

2. Many of the world's top cybersecurity experts advise businesses to operate under the assumption of an existing breach. That's why using a tool to discover an existing breach is critical. And it's what the SaaS Cybersecurity Assessment provides for SaaS applications, which are arguably the most important components of business productivity.

3. Encourage the prospect to visit your website so they know you're a legitimate business. If you have business reviews or testimonials from customers, encourage them to visit those areas of the site for further validation. If you've earned awards or have certifications that could be meaningful to the prospect, share those as well.

4. To add an additional layer of trust, encourage them to visit the SaaS Alerts website as well. This will demonstrate that SaaS Alerts is also a legitimate business that works with MSPs like yourself. In the footer of the SaaS Alerts website, there's an "Assessment" link that provides additional information around the value of the assessment and provides instructions on how the prospect can further validate you as an MSP through SaaS Alerts, if desired.

5. After the prospect has completed their detective work and is comfortable moving forward, it's time to send them an email with the link to the SaaS Alerts provisioning process. Let them know in advance that they'll need their admin credentials, but the process takes less than 90 seconds.

6. When you send them their provisioning email, consider providing them a unique code such as, "May the Force Be with You." Tell them you'll call them in a few minutes to verify the code in the email before they click through to anything and share their admin credentials. You, the MSP sales representative, will repeat the code back to them on the phone to validate that they are in fact clicking on a legitimate email that was sent by you. Throughout this process, you're demonstrating to the prospect that security is of the utmost importance to you.

7. After validating the unique code, walk the prospect through the 90 second provisioning process. After the prospect enters their credentials (which you, the MSP will never see), data from the prospect's SaaS applications will start to flow into the SaaS Alerts platform. Depending on the size of the environment, it may take up to 3 hours to provide a full picture of the environment going back 7 days, with 30 days of file sharing data.

8. Schedule a meeting to review the SaaS Cybersecurity Assessment with the prospect in the coming days.

9. **Close that deal!**

UPSELL YOUR EXISTING CUSTOMERS

Have customers that are hesitant to upgrade their services to the next level or add on SaaS monitoring for an additional fee? The same process can be used to help them see the security holes that may be lurking in their SaaS applications.

QUARTERLY BUSINESS REVIEWS

Quarterly business reviews (QBRs) are a great opportunity for MSPs to demonstrate the value they provide for their customers. The key is providing meaningful information to the business leader about the attack vectors that threaten their business and the steps taken by you to mitigate those threats.

With so many companies using SaaS applications to run their business, a QBR conducted by an MSP without insightful security and user behavior data around SaaS applications is simply incomplete. SaaS Alerts' reporting capabilities allow you to provide your customers with the following insights:

- Brute force attacks
- Suspicious file sharing data
- Employee data exfiltration activity
- Security, user, and admin policy changes
- New devices added
- Plus nearly 30 more events

Running a comprehensive and easily digestible SaaS Cybersecurity Assessment using SaaS Alerts takes only minutes and demonstrates to your customers that their "SaaS is Covered."

For questions or additional guidance, please contact your dedicated account manager or email sales@saasalerts.com.

SaaS Alerts™