Security Awareness Training

Buyer's Guide

How to use this guide

As a reference to confidently choose the right Security Awareness Training (SAT) platform without wasting time, money, or any remaining sanity. It covers **what matters** for MSPs (you), **what to avoid**, **how to compare vendors**, and **what to ask** before making a decision.

Find what you need:

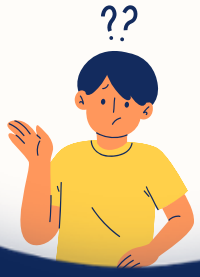
Click a section to skip ahead.

PHIN

1

Why does SAT matter?

If you're reviewing SAT platforms, we'll assume you already understand the fundamentals. **Human risk continues to be the biggest gap**, and the industry is not slowing down. Compliance pressures rise every year and **insurers want proof that your clients are not a liability** - regardless of their security background or technical abilities.



of breaches involve the human element
2025 Verizon DBIR

Here is the quick refresher:

- Human error remains the **number one cause** of breaches.
- Training supports **compliance requirements**.
- Better security behavior **reduces ticket volume and the risk** of real incident response work.*
- Strong SAT protects reputations, contracts, and cash flow.**

**AKA saves you and your clients time & money.*
***Again, saves you and your clients time & money.*

But you already know why SAT matters for your clients. **So, let's move onto what actually matters for you...**

2

What are your pain points?

Most SAT platforms weren't built for MSPs. They were built for internal IT teams then retrofitted for the channel.

Here are the pain points we hear most often that may resonate with you:

- **Too much manual work.** If every campaign needs to be built, reset, and managed by hand, your team loses hours you cannot bill. If you can't manage everything from one central location and you find yourself jumping in and out of client accounts, or constantly updating user lists by hand, you're wasting time.
- **Weak reporting that doesn't prove ROI.** You need reports that help justify your value in minutes. Many SAT tools only give completion stats.
- **Content users forget by lunchtime.** If training is dull, behavior doesn't change. That puts your clients at risk.
- **Billing that ignores client fluctuations.** MSPs have clients with seasonal staff, growth spurts, and natural turnover. Your SAT vendor should handle that cleanly.
- **Integrations that don't make sense or are missing.** Your PSA is your central nervous system, every ticket that you have to create by hand, every client bill you have to update manually, and every platform alert that doesn't automatically make its way to your helpdesk is wasting valuable time.

Choosing the wrong platform creates ongoing operational drag. Choosing the right one removes dozens of small headaches that add up fast.

3

What to look for in an MSP-friendly platform

This is the core list of SAT features. **If a platform struggles here, it's unlikely to scale with you.**

Click a section to skip ahead.

Automation, Scalability, & Admin

If automation is weak, your team will lose time every month. **Time is money**, and when it's unnecessary busy work, time is also a big dent in your team's morale and job satisfaction.

- Look for tools that focus on one-to-many actions as a foundational principle, not a bolt-on
- Role based access for your team
- Automated training enrollment and reminders
- New tenant onboarding within minutes (not days or weeks)
- Tailored training campaigns that run without manual management
- Automated reporting
- White labeling, so your users know who's training them
- Bulk user management
- Bulk campaign creation and management capabilities

Integrations & Ecosystem Fit

Can your SAT tool play well with the other parts of your tech stack?

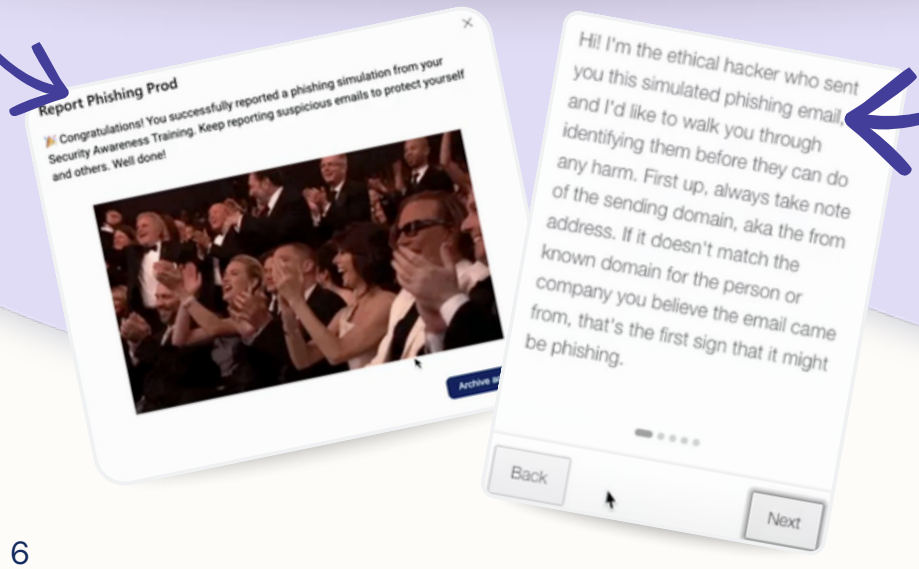
You need to consider everything that's already in place.

- PSA integrations
- Ticketing or alerting connections
- Marketplace availability through partners like Pax8 and Sherweb
- Resilient Microsoft and Google integrations for identifying users and training groups, and for sending traffic

End-User Experience

Everyone is incredibly busy, and your clients' employees are no exception. Good training should be relevant, short and easy for users to complete without putting it on mute and rolling their eyes. **The goal is to form better habits**, not bore your users to death and waste their time in the name of "compliance."

- Short, engaging modules
- A mix of available styles: live action, animation, and interactive content
- Options for different roles and risk levels
- Continuous updates, not a static library (ideally from multiple providers)
- Realistic phishing simulations
  - Templates that mirror current attacker tactics
  - Difficulty that increases gradually
  - Real time teachable moments instead of delayed generic content
  - Positive reinforcement for reporting suspicious emails



Reporting that Proves ROI

Reports should help you win renewal meetings and show progress clearly.

- High-level summaries that clients can understand
- Risk scoring or behavioral benchmarks
- Demonstrable improvement over time

Reports built for:

- QBRs
- Upsell conversations
- Cyber insurance submissions
- Contract renewals

Basically, you need to know whether you can justify your value to a client in less than five minutes using these reports - so **the metrics that matter include:**

- Users who need support
- Completed trainings
- Click rates on phishing tests
- Trends that tell a clear story

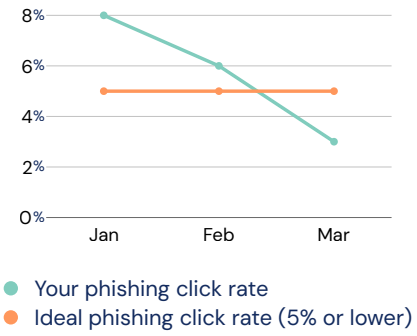
Sample QBR SAT Report

During Q1 2026, **you have decreased the likelihood of getting breached by a phishing email,** with your phishing click rate dropping from 8.2% in month 1 to 3.6% in month 3.

94% of your employees have completed all of their trainings. You need 100% completion for cyber insurance. **We recommend you [actions] to meet 100% completion.**

We need to **keep an eye on these users** who are most likely to click a phishing email:

- User 1, Click rate
- User 2, Click rate



Pricing Models

Pricing should support growth, not punish it. The wrong pricing structure can quietly erode margins or create friction every time a client adds or removes users.

Here's what to evaluate carefully:

- **Per-User vs Per-Tenant Pricing**
- **Minimum Seat Requirements**
- **Will you have to compete with your vendor when your client is up for renewal?**

Some vendors require minimum user counts per tenant. That can be painful for smaller clients or new accounts. If you support startups, seasonal businesses, or SMBs with fluctuating headcount, minimums can quietly eat into margin.

- **Flexibility for Growth and Churn**

MSP environments change constantly. New hires. Layoffs. Mergers. Rapid scaling. **A strong pricing model adjusts automatically to real usage** without forcing manual reconciliation or awkward conversations.

The right SAT platform should make it easier to scale revenue, not create accounting puzzles every month.

Red Flag: Pricing models that look attractive at small scale but become restrictive as you grow.

4

Ask your vendors...

There are a boatload of SAT vendors you can buy from, but some might steal your clients, charge you for licenses you don't use, or make it difficult for you to get access to your clients' environments. Maybe even all of the above.

To ensure you don't get stuck with the wrong provider, here are some questions you should ask before signing a contract:

- How long does it take to onboard a new client?
  - Can we do this on our own?
  - Does billing update automatically or does it require a new contract?
- How much time do most of your MSPs spend managing the platform once it's set up?
- Can you explain how your platform is multi-tenant?
  - Can I run and/or edit campaigns across multiple clients at once? What about keeping them separate?
- How do you handle user count changes month-to-month?
- What do MSPs our size usually struggle with?
- How often is your training content updated?
- Am I responsible for updating campaigns when new content comes out?
- What does your contract renewal process look like?
- Does phishing simulation difficulty progress naturally?
- What do end-users experience if they click a phishing simulation?
- What do your reports include and how do they explain the value of your SAT to our clients?
- If Buzz Lightyear doesn't know he's a toy in the first Toy Story movie, why doesn't he move when humans are around?

The goal: Separate marketing buzzwords from real capability.

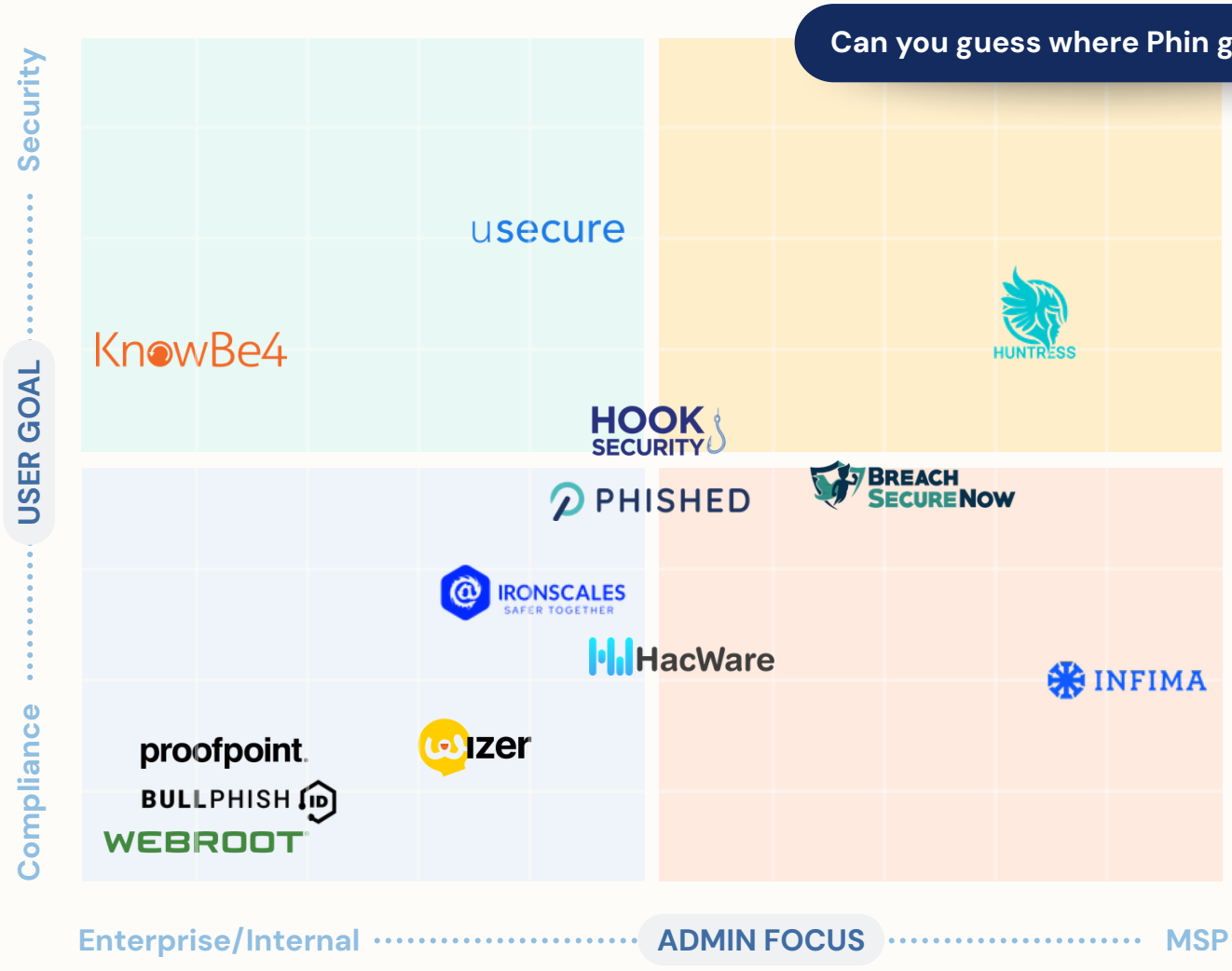
5

Who meets your needs?

Some providers are great for just checking a box while others strive for better security by genuinely changing user behavior. And when it comes to admin, platforms built for enterprise, probably won't work well for you (and vice versa).

This quadrant helps categorize vendors based on:

USER GOAL: *Training quality, variety, quantity, relevancy, recency, and frequency.*
ADMIN FOCUS: *Tenancy structure, integrations, billing, and automation.*



Return to top

6

Look out for these red flags

Avoid platforms that create more work than they save. You probably already know that, but you might benefit from a few tips on how to spot them!

- Long-term contracts that lock you in (especially when billing isn't usage based)
- Billing terms and a renewal process that don't sound ideal for you
- Workflows that require constant attention
- Single-tenancy disguised as "multi-tenancy"
- Training that treats every client and user the same
- Reporting that focuses only on training completion and doesn't give visibility into behavior trends
- Rare or slow content updates

If these appear early in your evaluation, you're gonna feel them even more once deployed.

7

How to prove the value of SAT to your clients

Your clients don't care about jargon – in fact, for most it will actively put them off. They care about staying operational, meeting insurance expectations, and avoiding costly downtime.

Here are simple ways you can communicate SAT so clients understand the value immediately.

Sell Outcomes

- Focus on risk reduction
- Highlight visible improvements
- Position training as a strategic part of a security plan
- Reinforce audit readiness and insurance benefits

Learn how to talk about it

Know What SMBs Care About

- Fewer chances of business disruption
- Keeping a great reputation among customers
- Avoiding compliance fines and losing insurance coverage
- Fewer panic tickets and mistaken reports

How to explain SAT to your clients

Client-friendly ways to sell SAT based on desired outcomes

- "In order to maintain your cyber insurance policy, we need to put a program in place."
- "Having SAT can reduce your chance of a breach, which reduces the chance of your business being shut down, held for ransom, and/or losing key data and $$$."
- "Your reputation can take a huge hit if it undergoes a cyberattack which means you could lose clients. But good SAT can reduce the risk of that happening."
- "Implementing SAT will help you get full cyber insurance coverage and avoid potential compliance fines."
- "The better your users are trained on phishing and other common hacking methods, the less likely they'll be to waste time making false reports, and the more likely they'll be to identify real threats to your business."

SAT is like a life vest

1. You wear it *before* something bad happens
2. It's simple, but extremely effective when worn properly
3. It's saved even the strongest of swimmers
4. It only works if it's on (not under the seat)

How to respond to pushback

You know the whole, "We're too small to get hacked." "No you're not, you're just too small to make the news." Well here's a few more to use when clients are feeling a little stubborn:

"Our users don't have time."	"It takes less time to train than it does to deal with a breach. And the training is just a few minutes a month. Small doses work better than long annual lectures."
"We haven't had an attack. We'll be fine."	"Most breaches happen to businesses that thought the same thing. Anyone, anywhere in the world with $5 in their pocket and an internet connection has recently gained access to powerful AI tools. Attacks are getting better, and we are seeing exponentially more of them. You need layered defense, and this is a crucial piece of it."
"Our users aren't dumb, they can tell when it's a scam."	"It's not about being smart or dumb. It's about making it a habit to reduce distractions and not make exceptions. Even the best cybersecurity experts have made just one mistake that haunts them."
"Don't we have tools to protect us?"	"Yes, but they aren't foolproof. They make attacks harder but not impossible, and 60% of breaches are caused by a human mistake."

8

Your Next Steps:

Choosing the right SAT platform is about **fit, long-term impact, and ease of use**. It should support your team, serve your clients, and strengthen your overall security posture.

- Match the tool to your **top operational challenges**
- Review reporting from the **perspective of a real client meeting**
- Confirm that **automation removes work** instead of adding it
- **Test the content** to ensure the user experience is simple and worthwhile (If you think it's bad or boring, your clients will too)
- Look for vendors that have a clear roadmap and **listen to your feedback**

Is PHIN the right partner for you? *Let's find out!*

Start your free trial | Schedule time

Return to top