

A Buyer's Guide for Security Awareness Training

How to Choose the Right SAT Solution for Your Business

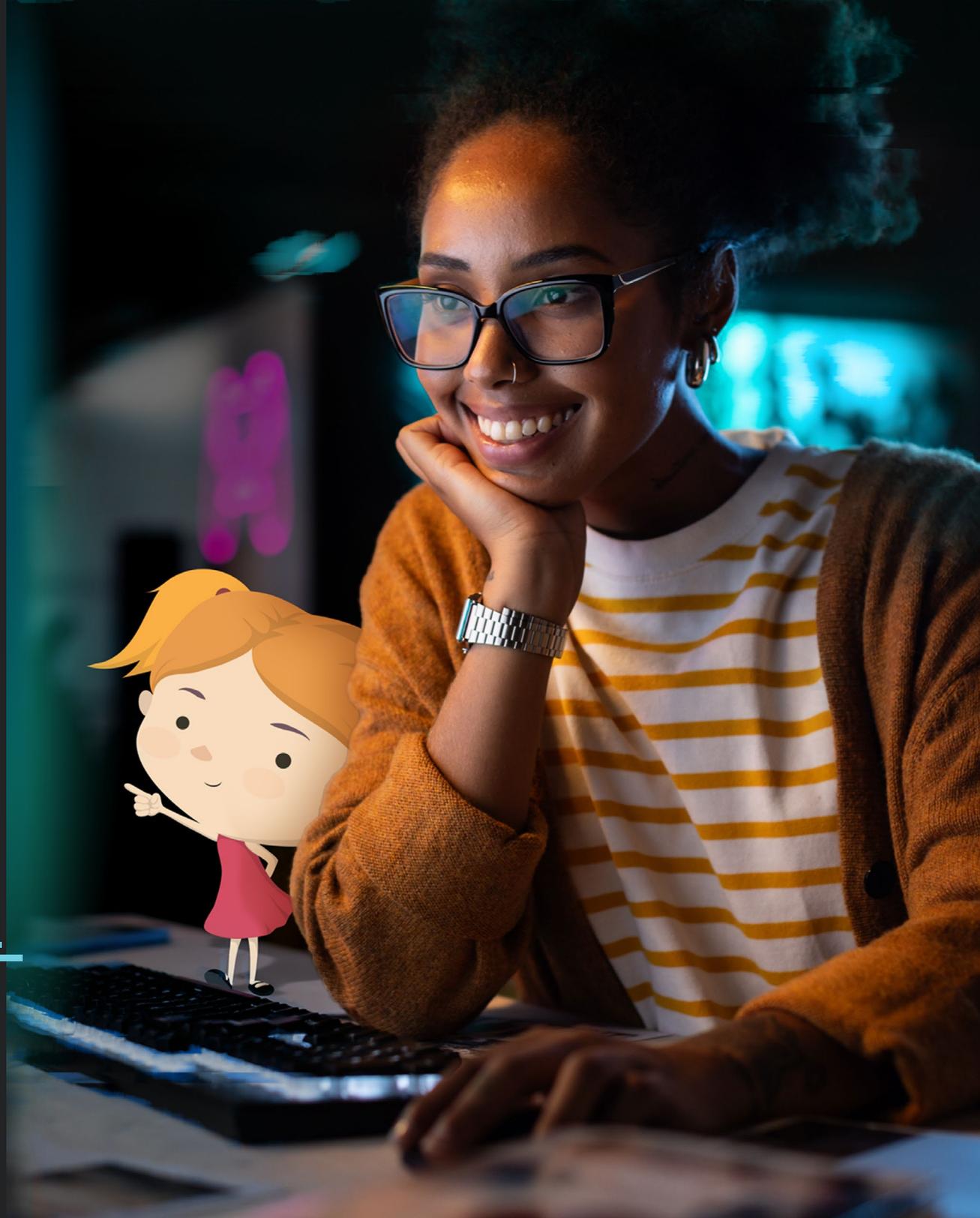


Table of Contents



Introduction Securing the Human Vulnerability	3
What Is Security Awareness Training (SAT)?	4
Age-Old Challenges of Old-School SAT	5
Building a Culture That Values Security Can Be Quite Easy	7
Ask the Right Questions Before Choosing Your SAT Solution	8
Essential Features of an Effective SAT	9
Huntress Security Awareness Training	13
The Threat Landscape is Changing. Your SAT Should Change With It.	18

Introduction

Securing the Human Vulnerability

There's a natural human desire to avoid threatening scenarios. The irony, of course, is if you hope to attain any semblance of security, you must always remain prepared to confront those very same threats.

As a decision maker for your organization, you know this well. But no matter how many experts or trusted cybersecurity tools your organization has standing guard, you're only as secure as your weakest link. There's still one group that can inadvertently open the gates to unwanted threat actors—your own people.



Security Must Be Second Nature for Your First Line of Defense

For your organization to thrive, you need capable employees. After all, they're your source for great ideas, innovation, and ingenuity. However, they're also human. And humans are fallible. Hackers understand no one is perfect, and that's exactly what they seek to exploit.

This is why your people have to become your first and last lines of defense against cyber threats. But to do so, they need to learn how to defend themselves against the treachery of hackers. That's where security awareness training (SAT) comes in.



The SAT Market is Overflowing, but Navigating it Shouldn't Overwhelm You

Not all SAT solutions are created equal. This is made evident by a jam-packed marketplace full of program options, leading to confusion on which ones are most effective and easiest to manage. That's why this eBook exists. If you need help understanding what to look for, we've got you covered.

The following pages help you understand the different approaches to SAT, how to build a culture around security awareness, and how to select the right solution for your organization.

84%
of cybersecurity leaders want to mitigate risk by managing employee behavior, yet few deploy effective solutions.¹

¹ Candrick, William, Richard Addiscott, Andrew Walls, and Alex Michaels. 2022. Innovation Insight on Security Behavior and Culture Program Capabilities. Gartner.

What Is Security Awareness Training (SAT)?

No business wants to fall prey to cybercrimes. The financial burdens alone can debilitate your entire operation. And that's why SAT exists.

The overall objective of a SAT program is to keep your employees and organization secure. The underlying benefit, however, is demonstrating compliance. While content may differ from program to program, most are generally similar, requiring your employees to watch scripted videos, study generic presentations, and take tests on cyber "hygiene."

At their core, SAT programs are designed to help you:

 Teach employees to spot cyber threats like phishing, social engineering, and ransomware

 Minimize your organization's exposure to cyber threats

 Maintain regulatory compliance with cyber insurance stipulations

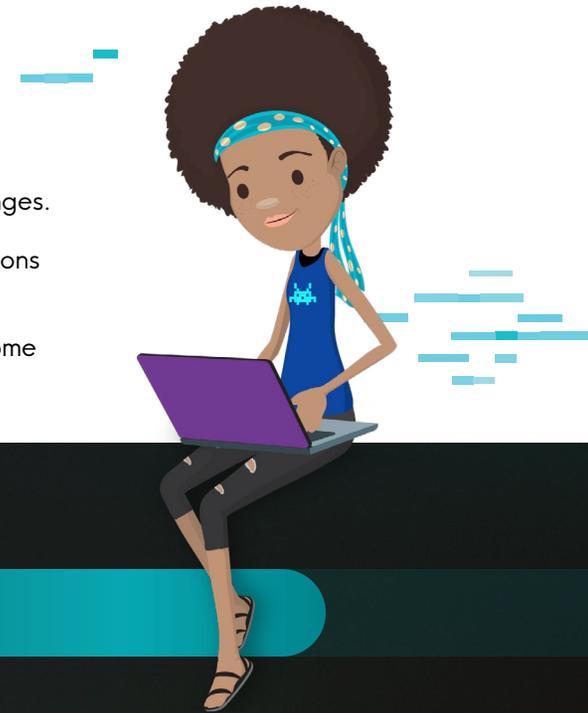
These are all worthwhile goals in helping your organization thrive amidst ever-evolving cyber threats. However, attaining these outcomes can feel like a pipe dream. That's because of one unfortunate truth about most old school SAT programs: **they dont work!**

So what separates an effective solution from an ineffective one? Before diving into what an impactful SAT program can look like, let's first understand why most don't work.

Age-Old Challenges of Old-School SAT

Traditional SAT programs have long been scrutinized for their inability to drive meaningful behavioral changes. If you oversee cybersecurity for an organization, then you're likely familiar with the pain that comes with implementing one, managing it, and encouraging its usage. Given their complexities, traditional SAT solutions practically force non-technical employees to become full-on technologists.

So what initially seems like a simple solution to "check the box" for compliance purposes can quickly become an ongoing headache, not just for you, but for everyone across your organization.



80% of all cybersecurity functions have less than one full-time employee dedicated to SAT.²

69% of employees admit to "intentionally bypassing" their enterprise's cybersecurity guidance.²

² Candrick, William, Richard Addiscott, Andrew Walls, and Alex Michaels. 2022. Innovation Insight on Security Behavior and Culture Program Capabilities. Gartner

Challenges for Administrators

Complex management and poor results

- Internal cybersecurity expertise needed to operate and manage SAT program
- Frustrating, manual onboarding
- Continual, time-consuming management
- Lessons assigned at infrequent intervals, leading to little positive change in your overall security posture

Challenges for Employees

Tedious, unengaging content

- Boring content isn't memorable
- Lessons aren't updated to current threats, so learners can't apply lessons to real-world situations
- Repetitive, outdated lessons negatively affect learning
- Sporadic, infrequent training fails to keep security awareness top of mind
- Employees perceive SAT as a time-consuming hindrance against other business needs

Challenges for Your Organization

Lack of efficacy

- Focus is more on helping you check a box for compliance purposes
- Many are designed with little reporting capabilities, leading to no visibility into success rates
- Most programs are created by generalists, not real cybersecurity experts
- Lessons rarely keep up with the current threat landscape
- Fail to instill meaningful behavioral changes that minimize risk for your organization

Building a Culture That Values Security Can Be Easy

The shared values, routines, and behaviors embraced by individuals across an organization are also known as its "culture." Typically, these norms are inspired by those in leadership. Therefore, if decision makers like you are the first to prioritize smarter cybersecurity habits, then it becomes easier to influence everyone else to adopt a culture that values security.

A key step in accomplishing this is introducing a SAT program that's:

- ✓ **Easy to deploy**
- ✓ **Easy to manage**
- ✓ **Easy to learn**

These three points are crucial to transforming your security posture. Because most SAT programs are complex to manage, they're usually dismissed as a means to an end. Just check a box for compliance and move on. But when done right, SAT can be an incredibly powerful tool to help your employees make smarter, more instinctive security-conscious decisions.

When you introduce a SAT program that delivers ease for you and your employees, it's more likely to become a welcome addition, ingraining a security-first mindset into the cultural fabric of your organization.



Ask the Right Questions Before Choosing Your SAT Solution

Building a culture around security entails embracing SAT. When it comes to choosing the right solution for your organization, however, there are some questions you should first ask yourself.

By assessing the following, you'll be better equipped to select the option that best fits your specific needs.

Your ideal SAT will allow you to answer a resounding "Yes" to all of the below.



Learning-Based Questions

- Are the lessons updated regularly to reflect current threats and scenarios?
- Does this SAT engage users in a unique, meaningful manner?
- Is this SAT built and supported by real cybersecurity practitioners?
- Is the teaching methodology proven to increase knowledge retention?
- Are the topics covered in this SAT relevant to my organization's security and compliance concerns?

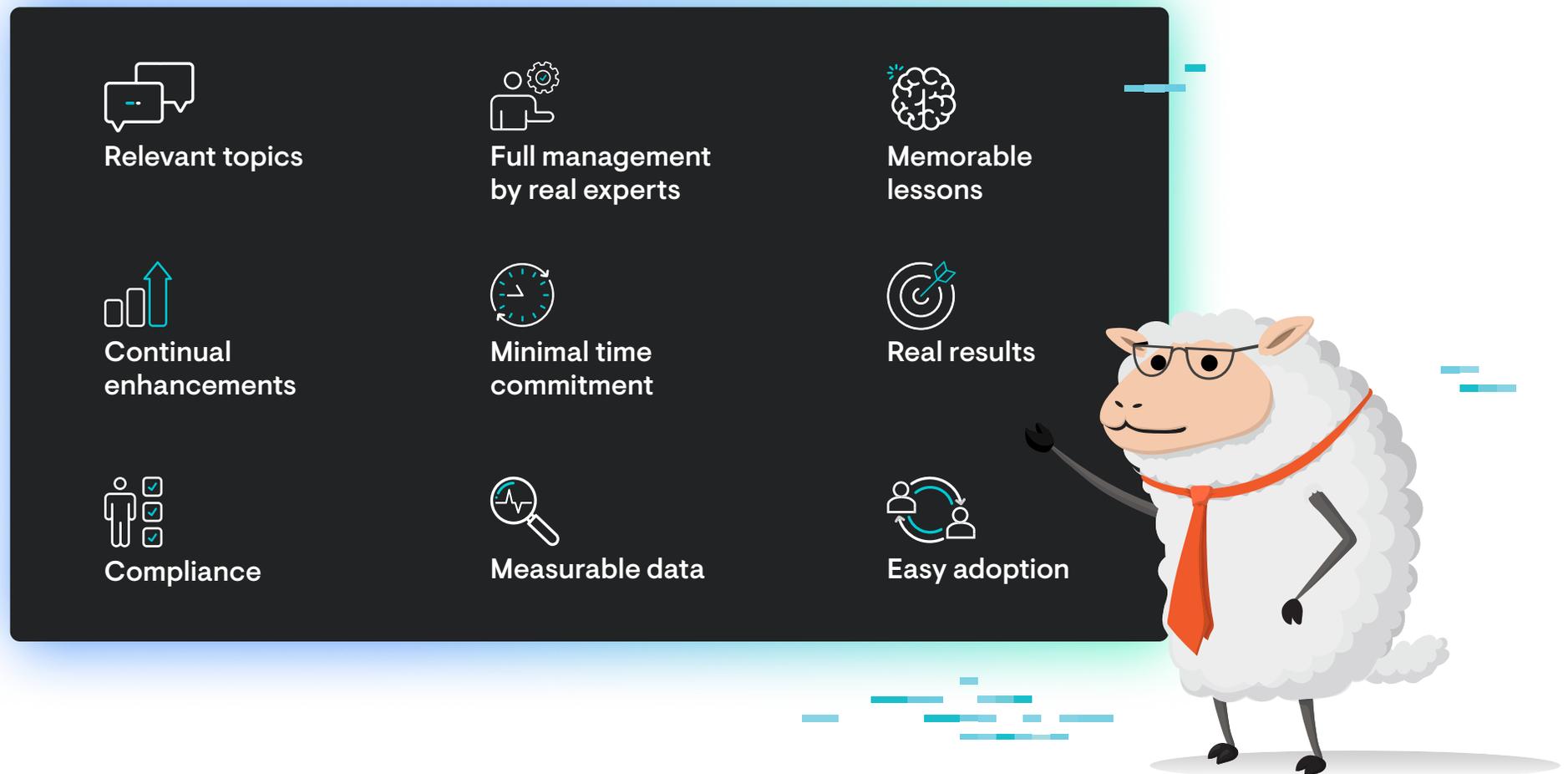


Management-Based Questions

- Can I reduce the burden of management without sacrificing quality?
- Can it be deployed quickly?
- Does it automatically enroll new users and automate management?
- Is it smart enough to skip non-human identities so I don't assign training to, say, our copy machine?
- Is it simple and intuitive enough for anyone across my organization to use?

Essential Features of an Effective SAT

A SAT solution that's easy to deploy, manage, and use can have a huge positive impact. That's because a solution that delivers "ease" has considered all of your organization's cybersecurity needs in advance. In other words, an effective SAT does all the heavy lifting on your behalf, as it features:



The image shows a cartoon sheep character with white wool, wearing glasses and a red tie, standing to the right of a large blackboard. The blackboard lists nine essential features of an effective Security Awareness Training (SAT) solution, each accompanied by a white icon. The sheep is pointing towards the blackboard with its right hand.

- Relevant topics**: Icon of two speech bubbles.
- Full management by real experts**: Icon of a person with a gear.
- Memorable lessons**: Icon of a brain with a starburst.
- Continual enhancements**: Icon of a bar chart with an upward arrow.
- Minimal time commitment**: Icon of a clock face with a circular arrow.
- Real results**: Icon of a target with an arrow in the bullseye.
- Compliance**: Icon of a person with three checkmarks.
- Measurable data**: Icon of a magnifying glass over a pulse line.
- Easy adoption**: Icon of two people with circular arrows between them.

Relevant topics

...based on real threats you and your team might encounter.

To avoid pre-canned, outdated training, choose a SAT solution that's backed by experts. Cybersecurity practitioners should be the ones regularly creating and updating lessons based on the latest trends they see hackers leveraging in the wild. Additionally, every lesson should cover a unique cybersecurity topic that reflects the most recent real-world tradecraft.

Full management by real experts

...so you don't have to waste time creating, managing, and assigning trainings.

Ideally, you want a SAT solution that can manage all necessary tasks for you. Seek a SAT solution that's backed by real cybersecurity experts who can create, curate, and deploy your learning programs and phishing scenarios on your behalf.

Memorable lessons

...with fun, story-driven episodes that are relatable and easy to comprehend.

Strive for a SAT solution that features character-based narratives. This indicates the SAT is carefully designed to engage learners of all attention spans. Keep in mind, if the lessons are intentionally entertaining and whimsical, you're more likely to find your employees conversing about inside jokes, recurring characters, and, of course, what they've learned. As a result, these ongoing discussions only serve to fortify your culture of security.



Continual enhancements

...so lessons are updated regularly in response to real-world threats.

Seek out a SAT solution that provides monthly lessons, as this will keep your learners up to date. Regular encounters with simulated cybersecurity scenarios can help enhance their abilities to spot and defend against risks, such as phishing attempts. These simulations should also be dispersed at unpredictable time intervals (i.e. morning, night, weekends, early in the month, later in the month, etc.), keeping learners on their toes and allowing them to put their security knowledge into practice.

Minimal time commitment

...your learners can complete their lessons in minutes. And you don't have to invest countless hours managing it all.

For your learners, choose a SAT solution that doesn't feel like an arduous chore. Look for solutions that specialize in engaging lessons that are designed to be completed in shorter periods of time.

For your own administrative needs, select a SAT that can sync regularly with your most popular platforms, such as Microsoft 365, Google, Okta, or Slack. It should also sync your employee directories with ease, so whenever you activate or deactivate users, it'll automatically update the information. Finally, make sure it's intelligent enough to decipher between human and non-human identities, so you're only charged for accounts linked to real individuals.

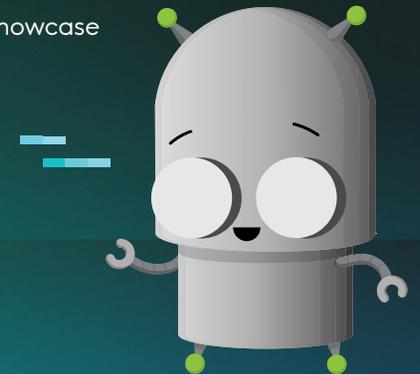
Real results

...through lessons that instill meaningful security-focused behaviors and habits.

An impactful SAT should deliver monthly training that's rooted in science-backed teaching methodologies proven to help your employees internalize and retain lessons better.

Your SAT should feature engaging videos, text, and short quizzes that showcase realistic cyber threats commonly encountered in the wild, such as:

- Phishing
- Social engineering
- Physical device security
- and more



Measurable data

...with easy-to-read reports on usage and success rates.

An impactful SAT program should provide robust reporting. Comprehensible summaries should highlight those employees who haven't taken their training or those who've been compromised by a phishing simulation. Additionally, detailed reports should give you all the data you need to help prove business, insurance, and regulatory compliance.

Easy adoption

...that makes it easy to deploy and easy to scale with your organization.

Choose a SAT solution that's specially built to accommodate organizations with limited time and resources. A solution that's easy to implement can be deployed across your organization in a matter of minutes.

An added bonus is if your SAT includes intuitive custom content creation tools. These can allow you to build your own unique training modules by uploading videos, creating quizzes, and assigning lessons for just about anything—from new hire onboarding to internal updates to team training and beyond.

Compliance

...with a range of standards and regulations

While compliance is the bare minimum of what a SAT should offer your organization, it shouldn't be understated. Whether it's to meet insurance check boxes or critical industry regulations, every business has its own compliance demands. At the very least, your SAT solution should cover the requirements of:

- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI)
- Service Organization Control Type 2 (SOC 2)
- EU General Data Protection Regulation (GDPR)

Huntress SAT—Built for Everything You Love. And Everything Hackers Hate.

Designed and managed by the trusted cybersecurity experts of Huntress, Huntress SAT takes a unique approach to security awareness training. It's easy to deploy and operate, so unlike other SAT solutions, you don't need a PhD in cybersecurity to use it. Better yet, it fuses vibrant animations with science-based learning principles to help improve your security posture, all while freeing you from the burden of complex management.

Simply put, Huntress SAT goes beyond the compliance check box—it leads to real results.



Admins Love It

No ongoing management
required

- Deployment typically takes minutes
- Integrates easily within your security stack
- Provides robust automated reporting
- Directory syncs automatically with your active and inactive users
- Custom Content Creator Tool allows you to modify, build, and personalize lessons
- Delivers measurable data on users' performance
- Syncs with Microsoft 365, Google, Okta, Slack
- Covers a range of compliance regulations, including HIPAA, PCI, SOC 2, GDPR

Learners Love It

Lessons are fun, engaging,
and memorable

- Episode-based lessons are full of eclectic, vibrant characters
- Lessons are relevant to modern cybersecurity threats
- Features story-driven narratives created by award-winning animators
- Utilizes neuroscience principles proven to help learners retain knowledge better
- Engaging content promotes ongoing discussions, helping reinforce your culture of security
- Episodes are easy to understand

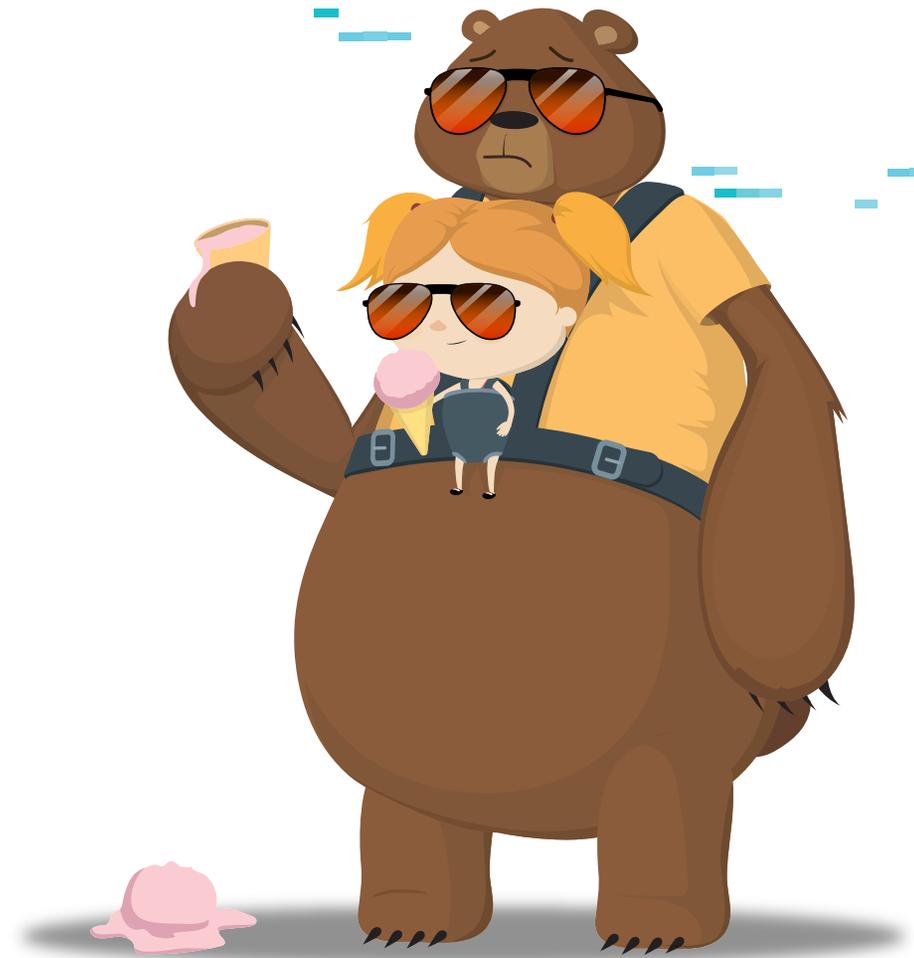
Hackers Hate it

Backed by real cybersecurity
experts

- Huntress experts—who manage over 2M endpoints—inform our lessons and phishing simulations based on their observations in the field
- Huntress SAT is always based on real-world scenarios, empowering individuals to face today's threats with confidence
- Better knowledge retention by learners means they're more likely to thwart cyber threats and protect your organization from hackers

“ The updated onboarding process and Huntress-managed features are game changers for us. I just onboarded a client with 68 users in under five minutes. **Huntress SAT has my clients eager to do their training now. They are liking these characters and are actually learning.**”

Michael Ehlert
President, We Travel PC



“ Most of the training in HIPAA is very dry with a ‘check-the-box’ kind of mentality . . . I was looking for something different and was introduced to Huntress SAT. I loved this new idea with how to present this information . . . **Nothing compared to the inventiveness that Huntress offered with their training episodes.**”

Jared Couillard, CISSP
Senior Director, IT & Security Officer,
Cohere Health



The Threat Landscape Is Changing. Your SAT Should Change With It.

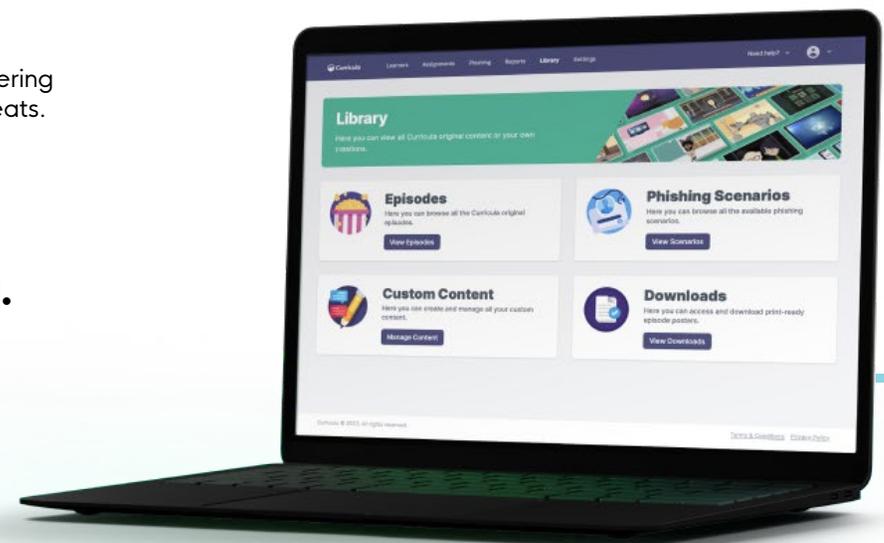
Cybercriminals think they're smart, maliciously targeting individuals across organizations like yours. That's why you need to ensure your employees are even smarter. If they're aware of the ever-changing tactics employed by hackers, they can stand as your first line of defense. But first, you need to deploy a training solution you can trust, one that's backed by real cybersecurity experts who understand emerging real-world threats.

Huntress SAT is the easy, effective, and enjoyable solution that helps:

- Minimize time-consuming maintenance and management tasks
- Improve knowledge retention through neuroscience-based learning principles
- Update you and your employees to the current threat landscape
- Establish a culture that values cybersecurity
- Inspire meaningful behavioral habits to improve security awareness
- Engage you and your employees in a creative, impactful manner
- Assure regulatory compliance
- Keep cybercriminals out of your organization

Discover how a fully managed SAT can free up your time and resources, all while empowering your employees with smarter habits that better protect your organization from cyber threats.

Say goodbye to ineffective, outdated training.
Say hello to Huntress SAT.
Start your [free trial](#) today.



About Huntress

Huntress is the leading cybersecurity partner for small- and mid-sized businesses (SMBs) and the managed service providers that support them. Combining the power of the Huntress Managed Security Platform with a fully staffed 24/7 Security Operations Center (SOC), Huntress provides the technology, services, education, and expertise needed to help SMBs overcome their cybersecurity challenges and protect critical business assets. By delivering a suite of purpose-built solutions that meet budget, security, and peace-of-mind requirements, Huntress is how SMBs defend against cyberattacks.

Founded in 2015 by a group of former National Security Administration (NSA) operators, Huntress has more than doubled over the past couple of years to protect more than 2 million endpoints, supporting 3,800 partners and more than 115,000 organizations. The company recently closed a \$60M series C led by Sapphire Ventures. For more information, visit huntress.com or follow Huntress on social media at @HuntressLabs on Twitter, Facebook, or LinkedIn.

Want to know more about Huntress SAT? Or just about Huntress in general? Simply reach out, and we'll be happy to answer any questions or help provide any support you might need.

[Contact Us](#)

