HUNTRESS

The Ultimate Buyer's Guide to Human Risk Management (HRM)

How to break through the noise and find the right HRM solution for your organization

Table of Contents

Executive summary

A Change is coming: The shift to HRM explained

Businesses have been pouring money into legacy security awareness training (SAT) for years. They've run the phishing simulations, users have sat through the painful hour-long lectures, and in the end, they've checked the compliance box they needed for cyber insurance.

So, with all this effort and training, why are human error incidents still on the rise? According to the Huntress report, Mind the (Security) Gap: SAT in 2025, 94% of security pros say incidents from human mistakes have shot up in the last three years. Even crazier? Over 60% say their organization's human risk exposure increased after rolling out SAT. And, based on findings from Verizon's 2025 Data Breach Investigations Report, breach data proves their point: in 2024, the majority of breaches (60%) involved some form of the human element.

Something is fundamentally broken.

And no, we're not saying that SAT is causing more breaches. But it's clear that the old way of doing things (infrequent, passive training for the sake of compliance) just isn't cutting it against today's threats. Hackers are getting smarter, and thanks to new tools like AI, their tactics are evolving at rates never seen before. If your security awareness training is stuck in the past, you're fighting a losing battle.

It's time to evolve.

Security professionals are shifting their focus from old school SAT to a more holistic, effective approach: **Human Risk Management (HRM).**

HRM isn't just another addition to the cybersecurity alphabet soup; it represents a fundamental shift in how we view and manage the human element of cybersecurity. It's about moving beyond simple awareness to identify and understand your risk levels, intervene when risky events occur, and drive impactful behavior changes that reduce those human risk levels.

In this guide, we'll walk you through the ins and outs of what HRM is, its impact on your organization, and what to look for in a solution that can finally turn the tide. Let's get into it.

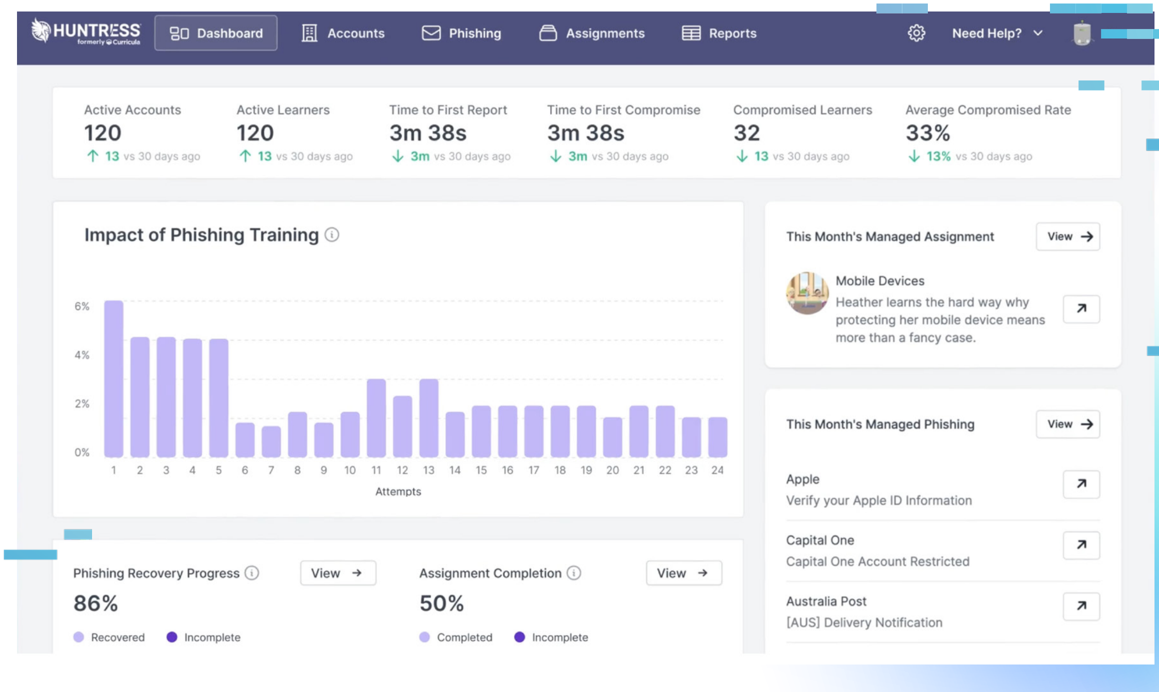
What to consider before you buy:

Moving from SAT to HRM

The SAT market is flooded with options that promise the world, but ultimately give you lackluster results. That's why a new category, Human Risk Management, has emerged. It's not just a rebranding of SAT—it's a necessary evolution. HRM is a comprehensive approach that focuses on identifying, quantifying, intervening, and actively reducing your human risk.

But don't throw the baby out with the bathwater. SAT is still an integral part of HRM. And when approached with a results-oriented mindset—instead of one that only helps you check a compliance box—it can have a major impact on your security posture, playing an integral role in helping you manage human risk.

But if you're stuck wondering what you're actually getting out of your existing SAT program, and looking for a change to make a real impact, here's what you should consider:



Active Accounts
120
↑ 13 vs 30 days ago

Active Learners
120
↑ 13 vs 30 days ago

Time to First Report
3m 38s
↓ 3m vs 30 days ago

Time to First Compromise
3m 38s
↓ 3m vs 30 days ago

Compromised Learners
32
↓ 13 vs 30 days ago

Average Compromised Rate
33%
↓ 13% vs 30 days ago

Impact of Phishing Training

This Month's Managed Assignment

Mobile Devices
Heather learns the hard way why protecting her mobile device means more than a fancy case.

This Month's Managed Phishing

Apple
Verify your Apple ID Information

Capital One
Capital One Account Restricted

Australia Post
[AUS] Delivery Notification

Phishing Recovery Progress
86%

Assignment Completion
50%

1. Can it actually help me understand my human risk?

Your current SAT program probably gives you metrics like completion rates and click rates from phishing simulations. Maybe even a vague "risk score" that doesn't delve into the details of what's behind it. But what do those numbers truly tell you about your human risk levels? Not much. They're merely a drop in the broader human risk bucket. A true HRM solution needs to go deeper.

Look for a solution that can:

Go beyond the basics:

Quantifying risk means looking at a wider range of behaviors and indicators. An effective HRM platform should help you detect and measure security behaviors outside of SAT vulnerabilities. For example, can the solution help you identify users with outdated browsers with critical vulnerabilities? An effective HRM platform should help you measure security behaviors and indicators, so you can understand your vulnerabilities and address them head-on.

Detect risky behaviors:

An effective HRM solution not only measures human risk but can detect risky behaviors as they happen, so you can intervene **before** they cause an incident. breach. For example, integrating with tools like **Endpoint Detection and Response** (EDR) or **Identity Threat Detection and Response** (ITDR) lets you flag a user who's storing passwords insecurely or has multi-factor authentication (MFA) disabled and provide them with appropriate training to mitigate that behavior. Think of it as an early warning system. You want to know who your riskiest users are so you can intervene before they cause a breach.

Provide clear risk quantification:

Whether it's a high/medium/low rating or a detailed scoring engine, the platform should give you a clear, quantifiable understanding of risk at both the individual and team level. This helps prioritize your efforts where they're needed most, and understand how these measures are performing.

2. Does it enable real-time, adaptive interventions?

Traditional SAT is static. Learners receive a training module, possibly a simulated phishing email, and complete it. Then, they move on. But what happens when real risky behaviors go down? What if you could turn them into teachable moments? Or, better yet, what if you could stop them before they even happen? That's where HRM's real-time, adaptive interventions come in.

Your HRM platform should offer:

Targeted intervention training:

Imagine your EDR or ITDR detects a user downloading a sketchy file. On top of stopping the threat, your HRM solution then automatically assigns a short, targeted training module on malware. This is the power of adaptive intervention. It's relevant, timely, and far more effective than a generic annual course.

Just-in-time coaching:

When a user **does click** on a simulated phish, what happens next? A slap on the wrist? A failing grade? Nothing at all? A better approach is immediate, personalized coaching. One that helps a user understand what went wrong in the moment, without threatening their psychological safety. Because a scared user is a user who will not report suspicious incidents in the future. So instead of "Remedial Training," look for "Coaching" features that explain **why** the email was a phish and what to look for next time. It turns a mistake into a powerful learning moment

Nudges, not nagging:

Sometimes, all a user needs is a gentle nudge. A quick message on Slack or Teams to review their cloud app permissions or update their browser can be incredibly effective at mitigating risks before they become a real problem. The key is to be helpful, not another annoying notification to be ignored.

3. Is the content engaging and based on real threats?

SAT isn't going anywhere, but it does need to evolve. Let's be honest, most SAT is long, boring, irrelevant, and infrequent. This type of training doesn't stick. And it definitely doesn't change user behaviors. In the Mind the Security Gap report, learners reported that they want interactive, hands-on activities and realistic examples of modern threats. Yet, 90% of employees say they encounter repetitive SAT content that offers no new insights. Hackers evolve too quickly to be training on old threats.

Instead, look for content that is:

Story-based and relatable:

Stories are one of the most effective ways people learn. They're engaging, easy to follow, and people can relate to the plots and characters. Good training uses stories to make complex and intimidating cybersecurity topics accessible and approachable to learners of any technical background. This means everyone comes away with new information and actionable steps to improve their security awareness.

Informed by threat intelligence:

The threat landscape is constantly evolving. Your training should, too. An HRM solution should leverage real-world threat intelligence from endpoints and identities across the globe to create training material and phishing scenarios that reflect what's actually compromising people in the wild. If your SAT is training for Nigerian prince scams instead of deepfakes or **business email compromise** (BEC), your learners are already years behind.

Interactive and hands-on:

Passive learning, where learners can click through without paying attention, isn't enough to change behaviors. And while phishing scenarios are helpful to reinforce training, most providers stop there. Look for a solution that goes beyond simple passive training and phishing scenarios by giving users hands-on reinforcement with a variety of tradecraft that could target them. When users interact with the tradecraft, they gain a deeper understanding of it. Bonus points if it can teach the "hacker mindset," helping to future-proof your users as they become better at identifying new threats.

4. Does it integrate with your existing security stack?

HRM isn't a silo. Its power comes from its ability to connect the dots between human behavior and security events. Many HRM providers require you to set up and manage 15+ integrations, which is a nightmare for lean IT and security teams.

The right solution should:

Offer seamless integrations:

Look for a platform that works with the tools you already use, like your EDR, ITDR, and Security Information and Event Management (SIEM). A vendor with its own integrated platform means you can consolidate and eliminate the headache of managing countless third-party connections.

Leverage integration for action:

The goal isn't just to pull in data; it's to use that data to trigger responses, interventions, and nudges. For example, an event in your EDR or ITDR should be able to kick off an intervention in your HRM tool automatically. This creates a closed-loop system for managing human risk.

GRC integrations:

While HRM outcomes should go beyond simply checking a compliance box, compliance is still a necessary part of it. Integrating with your Governance, Risk, and Compliance (GRC) tools is an easy way to automate the management of your policies, risk assessments, and regulatory adherence against common frameworks, freeing up time for more strategic security priorities.

5. Who's going to manage it?

Perhaps the most important question of them all: Who has time for all of this?

With most SAT programs, you get quarterly or annual training, and that's it. But threats don't operate on a quarterly schedule. The reality is that threats continually evolve, and admins can't keep up. The Mind the Security Gap report revealed that 72% of security admins feel that managing SAT is a burden. Over 60% of them say they're spending 10+ hours a month managing SAT programs that are often outdated, and 45% say keeping content updated is their biggest challenge. And this is just on SAT alone. Add in all the new functionality of HRM, with all the alerts, knobs, and levers that come with it, and suddenly you're in way over your head.

You and your team are busy enough with other security priorities. You don't have time to become full-time HRM administrators. Look for a solution that lifts that weight off your shoulders instead of adding to it.

Consider a fully managed service where:

A Security Operations Center (SOC) runs the program for you:

Imagine getting an entire team of security experts to manage your HRM program without adding any headcount. They handle content, simulations, monitoring, nudges, interventions, reporting, and other tasks. All while your team is freed up to focus on other priorities

You get expert oversight:

A managed service provides the senior-level security talent that most businesses can't afford to hire full-time. These experts provide the oversight and interventions needed to achieve real HRM outcomes.

Must-have capabilities in an HRM solution

Engaging and impactful training content built on real-world threat intelligence

Realistic phishing scenarios with post-compromise coaching

Hands-on training reinforcement for different types of tradecraft

Human risk detection, measurement, and quantification

Real-time, adaptive interventions

Integrations with your security and GRC tools

24/7 management by senior-level security experts

Fast time-to-value and easy deployment

Admin and learner-friendly experience

What do *you* want from your HRM solution?

The first step in figuring out what you want in an HRM solution is to find what you **need**. Use this list as a self-assessment starting point to clarify your priorities. Answering “Yes” or “No” will help you hone in on what you truly need and guide you toward an HRM solution that aligns with your goals.

Statement	Yes	No
We’re concerned that our current SAT doesn’t drive meaningful behavior changes.		
We need to identify and address human risk beyond SAT (e.g., insecure password storage, outdated browsers).		
We want business-level visibility into human risk levels and HRM performance.		
We’re overwhelmed by the management overhead involved, or we lack the expertise to keep training relevant.		
We need a partner that can handle Human Risk Management 24/7, even when we’re offline.		
We want a provider who can detect risky behaviors and risk indicators and provide interventions to correct them.		
We prefer human-led management and triage over purely automated training programs and alerts.		

How to evaluate your HRM needs

Choosing the right HRM partner means cutting through the buzzwords and getting clear on capabilities, coverage, and outcomes. Use this checklist to guide your process and check if your vendor is merely training users instead of **actually** reducing human risk.

Risk measurement and insights

- How does your platform measure and quantify human risk?
- Can you give me detailed insights at both the individual and team levels?
- Does your solution detect and track behaviors beyond phishing clicks, like insecure password storage or outdated browsers?
- How do you prioritize risks to help us address the most critical vulnerabilities?

Adaptive interventions

- Does your solution support real-time, behavior-based interventions?
- Can you automatically trigger specific training or responses to risky behaviors?
- How does your platform ensure that interventions are timely and relevant?
- Are coaching and just-in-time training included to address user mistakes as they occur?
- What types of user-friendly “nudges” does your solution provide to mitigate risks before they escalate?

Content quality

- Is your training content interactive, story-driven, and does it reflect real-world threats? What are examples of recent threats you’ve incorporated into your training?
- How often is the training content updated to align with the latest threat landscape?
- Do you include hands-on simulations to reinforce learning?
- How is the content tailored to meet the needs of non-technical users?

Integration

- Can your solution integrate seamlessly with our existing security tools like EDR, ITDR, and SIEM systems?
- Does the integration support automated interventions and create a closed-loop system for risk management?
- Do you offer other security tools like EDR, ITDR, or SIEM to help us consolidate vendors?
- Do you provide support for integrating the solution into our existing environment?

Management and support

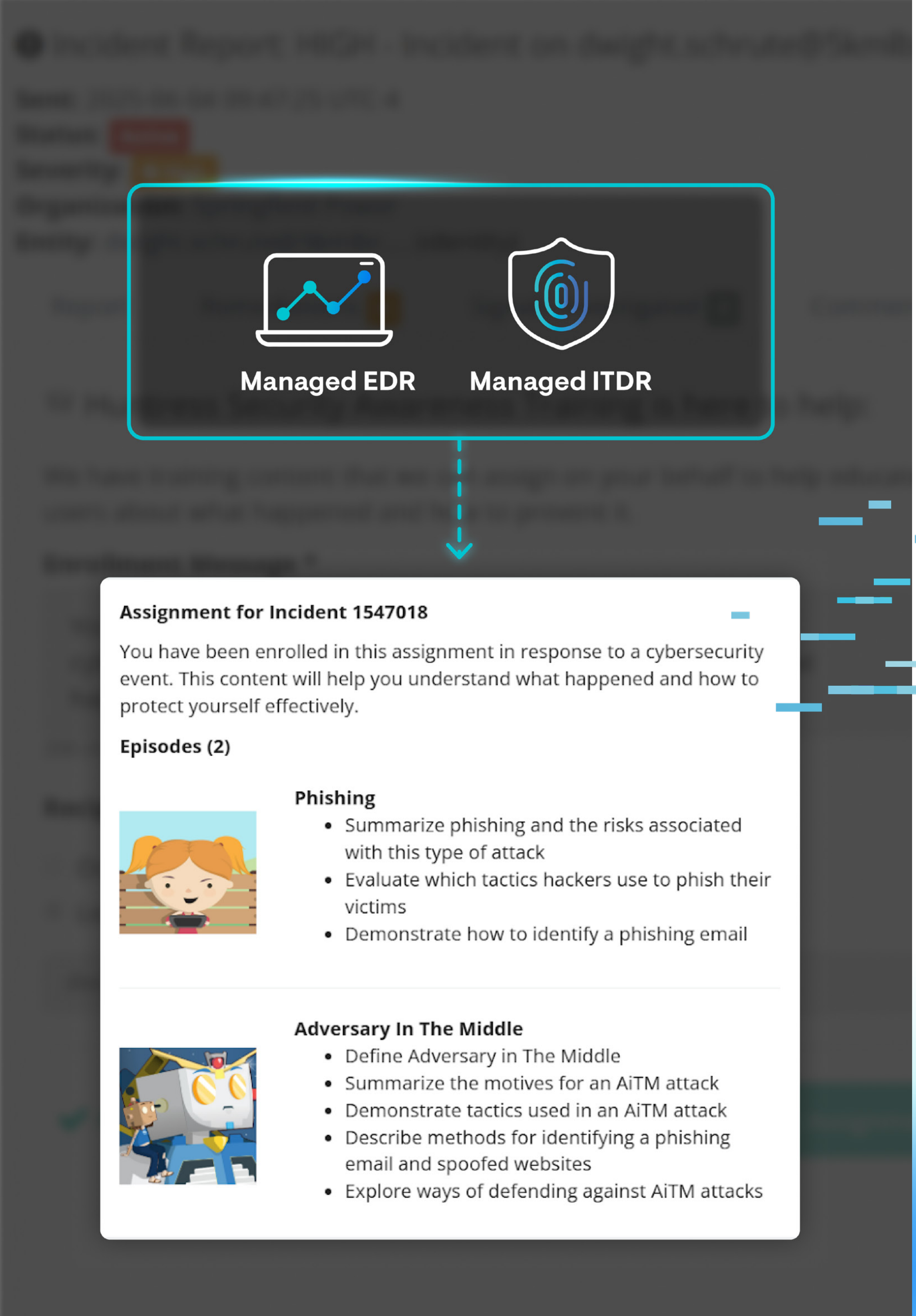
- Is this a fully managed service, or does it require dedicated internal resources to administer? How much time does your typical customer spend managing?
- What level of oversight and expertise does your team provide when managing the solution?
- Does the platform come with automated features to reduce ongoing administrative burden?
- How scalable is the solution as our organization grows or our security needs evolve?

Measurable outcomes

- How do you measure the success and impact of the HRM program over time?
- Do you provide reports that demonstrate improvements in risk reduction and behavior change?
- How does your solution help fulfill compliance requirements while driving real security outcomes?

Buyer's Checklist

Capability	Must-Have	Nice-to-Have	Not Needed
Provides 24/7 monitoring and management			
Delivers business-level metrics and visibility into human risk levels			
Measures, identifies, and quantifies risk beyond SAT activities			
Training follows adult learning frameworks to change behaviors			
Training is built on real-world threat intel to reflect today's threats			
Reinforces training with interactive modules for various tradecraft beyond phishing via email			
Has just-in-time coaching for simulated phishing compromise			
Includes nudges to preemptively correct risky behaviors			
Integrates and ingests data from other security tools			
Vendor provides other security tools to help with consolidation			
Integrates with your Governance, Risk, and Compliance tools			
Enables real-time, adaptive interventions for incidents			



Assignment for Incident 1547018

You have been enrolled in this assignment in response to a cybersecurity event. This content will help you understand what happened and how to protect yourself effectively.

Episodes (2)

Phishing

- Summarize phishing and the risks associated with this type of attack
- Evaluate which tactics hackers use to phish their victims
- Demonstrate how to identify a phishing email

Adversary In The Middle

- Define Adversary in The Middle
- Summarize the motives for an AiTM attack
- Demonstrate tactics used in an AiTM attack
- Describe methods for identifying a phishing email and spoofed websites
- Explore ways of defending against AiTM attacks

The road to HRM starts with Huntress Managed SAT

Plenty of vendors will label themselves as "HRM solutions," but the offerings on the market vary so widely that choosing the right one seems impossible.

Huntress gives you HRM in a way that makes sense for businesses that need to secure their people without the luxury of a Fortune 500 security budget. **Huntress Managed SAT** isn't just another training tool—it's a core part of a managed security platform designed to actually reduce human risk.

Here's how Huntress Managed SAT checks all the boxes:

It delivers true Human Risk Management, not just SAT

Huntress goes beyond simple awareness. Managed SAT helps you achieve true Human Risk Management by delivering effective, managed training that shifts behavior and is integrated with other security tools like our Managed EDR and ITDR to identify and mitigate risky behaviors in real-time.

Expert-backed and fully managed

Most organizations spend 10+ hours a month managing just their SAT program, and with the additional work required for HRM, the overhead can get out of hand fast. With Huntress, you'll get a team of world-renowned security experts managing your entire program for you. We build the training, run monthly learning programs and phishing campaigns, and give you the oversight needed to spot and stop risky user behaviors. You get the benefit of senior security talent on your side without the six-figure salary.

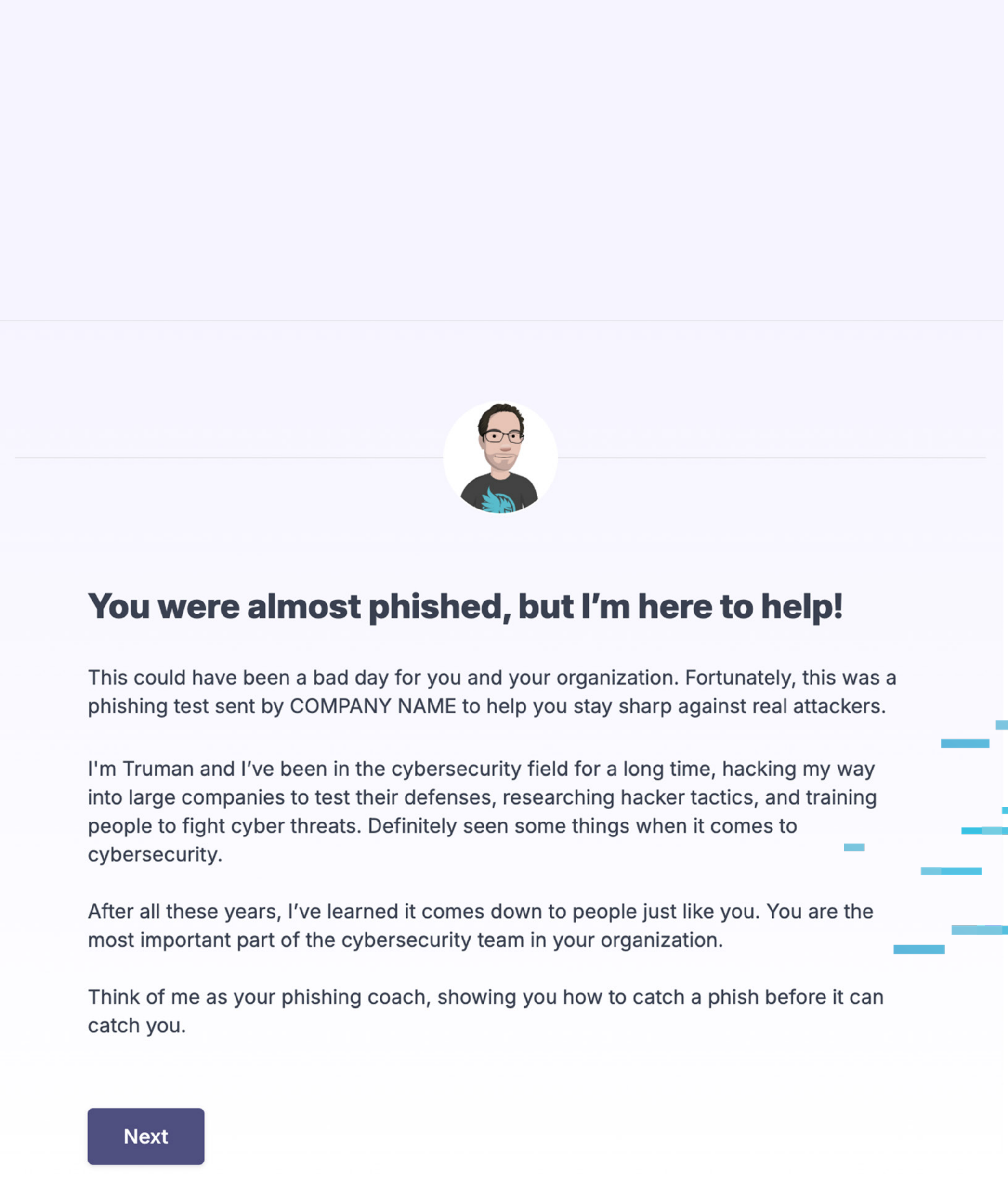
Engaging, threat-informed content

Our story-based, animated episodes are created by our SOC working alongside our team of adult learning experts and Emmy®-winning animators and adhere to proven adult learning frameworks. They're not just tolerable; they're genuinely engaging. More importantly, our content is fueled by real-world threat intelligence from the millions of endpoints and identities we protect, so all training is relevant to the current threat landscape. Your team will learn how to defend against the threats they're most likely to face today.

Experiential learner to reinforce training

Simple passive learning (things like videos, slideshows, and lectures) isn't enough to change user behavior. With Huntress Managed SAT, your users not only get engaging video content with quizzes interspersed to keep their attention, but also unique learning experiences:

- Realistic Phishing scenarios that include interactive, personalized **Phishing Defense Coaching.**
- The **Threat Simulator**, a one-of-a-kind learning experience that puts learners in the seat of a hacker to carry out simulated threats, teaching them to think like a hacker so they become better defenders



You were almost phished, but I'm here to help!

This could have been a bad day for you and your organization. Fortunately, this was a phishing test sent by COMPANY NAME to help you stay sharp against real attackers.

I'm Truman and I've been in the cybersecurity field for a long time, hacking my way into large companies to test their defenses, researching hacker tactics, and training people to fight cyber threats. Definitely seen some things when it comes to cybersecurity.

After all these years, I've learned it comes down to people just like you. You are the most important part of the cybersecurity team in your organization.

Think of me as your phishing coach, showing you how to catch a phish before it can catch you.

Adaptive interventions that drive change

Going beyond SAT means doing more than simple training and phishing. You need to be able to identify risky behaviors and intervene with the appropriate measures, whether that be nudges, relevant training, or policy changes. Here are some examples of how Huntress provides adaptive interventions for real risk indicators:

- **Behavior-Based Assignments:** Huntress Managed SAT integrates directly with our Managed EDR, ITDR. When an incident is triggered by a user's action, you can easily assign them targeted training based on the exact behavior that triggered the incident. So you can correct risky behaviors before they become a bigger issue.

- **Phishing Defense Coaching:** When a user is compromised in a simulation, they get instant, personalized coaching that helps them understand the red flags they could have looked for. We focus on a "coaching" approach for this just-in-time training to create the perfect "teachable moment" that doesn't shame the user for a mistake, but instead encourages them to look out for and report future incidents.

An integrated platform that just works

Forget about managing dozens of painful integrations. Huntress is a unified security platform. Managed SAT works seamlessly with our other products, providing unmatched visibility and response capabilities. This is how you build a security posture that's strong from the endpoint to the end user.

The time to act is now

Continuing to invest in legacy SAT leaves the door open for hackers to wreak havoc on your organization. The human element is involved in the vast majority of breaches, and it's time to address that reality head-on with a strategy that works.

Human Risk Management is the future, and Huntress Managed SAT is the simplest, most effective way to get there. It's managed for you by experts, beloved by learners, and integrated into a platform that delivers real security outcomes.

Ready to stop checking boxes and start reducing risk?

Learn more about Huntress Managed SAT and see how we can help you build a stronger human defense.

HUNTRESS®