usecure

Partner Playbook

An MSP's guide for selling
usecure's Human Risk Management

Table of contents

About usecure

The old-school approach to security awareness is broken, and the majority of user-focused solutions are worlds away from being 'MSP-friendly'.

We're on a mission to change that.

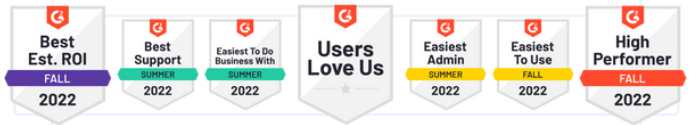
Founded in 2016, usecure is now embedded in the channel community, offering the leading human risk management (HRM) solution that is purpose-built for MSPs — and we're not done yet.

- Launched in 2016, HQ in the UK
- Built for MSPs, localised in 8+ languages
- Educating 100,000s of end-users
- 2022 finalist in the CompTIA 'Innovative Vendor' award

We're embedded in the channel community...

CompTIA
THE TECH TRIBE
channel program
MSPGeek

...and our users love us.



“

By 2024,

25%

of midsize enterprises will adopt security awareness training as a managed service, up from less than 5% in 2020.

Gartner

Market Guide for Security Awareness Computer-Based Training

The MSP opportunity

When it comes to information security, organisations of every size are starting to realise that inside threats are just as important as outside threats — and they’re starting to do something about it.

Spending on security awareness training products and services (including tools such as phishing simulators and advanced risk reporting) has grown rapidly in recent years and isn't slowing down anytime soon.

Cybersecurity Ventures predict that adoption will continue to grow rapidly, eventually pushing the security awareness training products and services market to be worth $10 billion annually by 2027.

Market trends

With most data breaches *still* originating from human error, the way the industry has addressed awareness training hasn't worked. The market is now offering a different solution for **managing human risk**, not just better ways to train people.

Old-school security awareness approach

- Tick-box driven, aimed at meeting compliance requirements
- One-size-fits-all training approach, often delivered sporadically
- Often judges risk based on course grades and completion rates

VS

New-school human risk management approach

- Aimed at building a security culture and driving secure behaviour
- Engaging micro-training, tailored to each users unique risk areas
- Ongoing risk is calculated through multiple data points

> The value proposition of most vendors is moving beyond content-heavy offerings to technology-heavy features to enable high user engagement and effectiveness.

Frost Radar™
Security Awareness Training Market

Key market drivers

The increased risk of digital adoption, poor security behaviour, evolving cyber threats and stringent compliance standards are encouraging decision makers to build a security culture.

Evolving threats

In 2021, 83% of organisations experienced phishing attacks and, in 2022, an additional six billion attacks are expected to occur. According to Verizon's 2021 DBIR, around 25% of all data breaches involve phishing.

Human error

According to the IBM Cyber Security Intelligence Index Report, 95% of cyber security breaches are primarily caused by human error, which is often the result of falling victim to a phishing attack or sharing credentials.

Digital adoption/remote work

People are on the front lines of potential security incidents every day, accessing sensitive data on multiple devices. Remote work means an employer has even less control and visibility over employees' data security.

Compliance standards

Security standards across the world mandate that businesses adopt stringent measures to prevent the data leakage of personally identifiable information (PII), including ISO 27001 and GDPR. Learn more >>

Why usecure?

usecure eliminates the ineffective and time-consuming nature of traditional security awareness training, offering a more complete human risk management solution that assesses, boosts and monitors ongoing employee security behaviour through admin-lite automation.

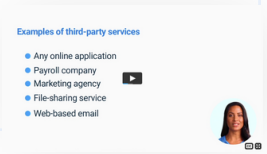
Our simplified approach sets us apart:

01 Evaluate

Assess employees' existing cyber risk areas through a quick 15-minute gap analysis assessment.

02 Educate

Strengthen user resilience with tailored training programs that prioritise courses to tackle each users' high risk areas first.

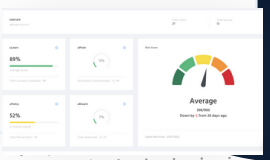


03 Calculate

Measure the training's impact and assess user security posture in other areas, such as dark web exposures. policies and phishing.

04 Demonstrate

Showcase your regular training efforts and policy processes to gain compliance with key security standards, like ISO 27001.



Key features

See usecure's key features in action

Explore MSP Demo Hub

uLearn

Security awareness training

- Automated user training
- Custom course builder (LMS)
- User-tailored programmes
- 100+ readily-made courses
- Ongoing training reporting

uPhish

Simulated phishing

- Automated phishing tests
- Custom template builder
- 700+ readily made templates
- End-user phish alert button
- Ongoing phishing reporting

uBreach

Dark web monitoring

- Dark web breach monitoring
- Identify exposed user accounts
- Locate the breached services
- Learn what data is exposed
- Dig down into user breaches

uPolicy

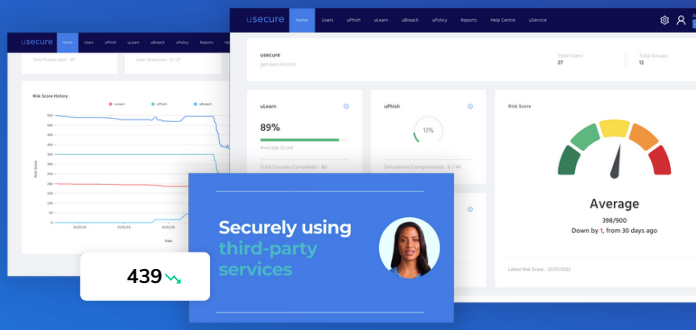
Policy management

- Automated policy approvals
- Centralised policy library
- Essential policy templates
- Edit and build custom policies
- Track outstanding signatures

Risk Reporting

Human Risk Analytics

- Company-wide human risk scoring
- uLearn, uPhish, uBreach and uPolicy performance
- Self-access employee risk profiles (End User Portal)
- Real-time reporting dashboard with key metrics
- Automated email summary reports for clients



usecure's differentiators

Simplicity is at the core of everything usecure does

Rather than relying on a content-heavy training offering which can often be time-consuming to run, usecure eliminates complexity through intelligent automation that crafts, deploys and manages measurable user-tailored HRM programmes in just a few steps.

Automation

Intelligent 'plug-and-play' automation makes usecure quick to deploy, easy to manage and pain-free to report on with features like AutoEnrol and AutoPhish.

Personalisation

Rather than relying on one-size-fits-all training, usecure deploys user-tailored training programmes that prioritise each individual's high-risk areas.

Customisation

With a custom LMS system and template editor, you can easily create custom courses and phishing emails that are unique to your business needs.

Comprehensive

usecure goes beyond user training, offering a full-circle solution for creating a security culture through uPhish, uBreach, uPolicy and risk analytics.

Flexibility

usecure offers flexible monthly billing with no minimum contract, making it easy for your clients to experience the value of usecure without commitments.

Support

We're big on support, offering hand-held onboarding, product tours, on-demand demos and around-the-clock live chat response in under two minutes.

The competition

View G2's latest competitor analysis

Latest Comparison

Independent reviews sourced from G2's 2022 Summer Report for 'Security Awareness Training'

	usecure	KnowBe4	Proofpoint
Meets requirements	97%	95%	92%
Ease of setup	96%	88%	87%
Ease of use	97%	91%	90%
Content library	92%	89%	80%
Phishing assessment	97%	94%	89%
Quality of support	96%	94%	91%
Risk scoring	87%	87%	81%
Continuous assessment	92%	90%	82%
Reporting	87%	88%	70%

How to package usecure

We recommend splitting your subscription options into two tiers - Core and Advanced. This helps keep your clients' options flexible, whilst keeping the platform simple to sell with an opportunity to increase your margins.

Plan	Service		Admin	RRP
Core *Launch an automated program in a flash and start demonstrating value*	**uLearn** Automated user training	**uPhish** Automated phishing tests	**Admin Time = Very Low** Automate everything! Set it and forget it Launch full program in a flash Great entry plan for clients who want to test the platform	**£2.50** per user/ per month USD = $3.00 AUD = A$4.50 EUR = €3.00 NZD = NZ$5.00
	uBreach Automated breach scans	**Reporting** Automated reporting		
Advanced *Enhance value and grow your margins, whilst keeping admin low*	**uPolicy** Policy management		**Admin Time = Low** Readily-made phishing and policy templates Easily build custom courses Distribute your custom content amongst other clients to save time	**£4.00** per user/ per month USD = $4.50 AUD = A$7.00 EUR = €5.00 NZD = NZ$8.00
	Custom phishing campaigns	**Custom** user training courses		

- **Core Plan** - is heavily automated, can be launched in a few clicks and takes minimal time to manage - making it a great starter plan to showcase usecure's value.
- **Advanced Plan** - is a great way to offer additional value and increase your margins, with a library of done-for-you templates that keep admin incredibly quick and easy.

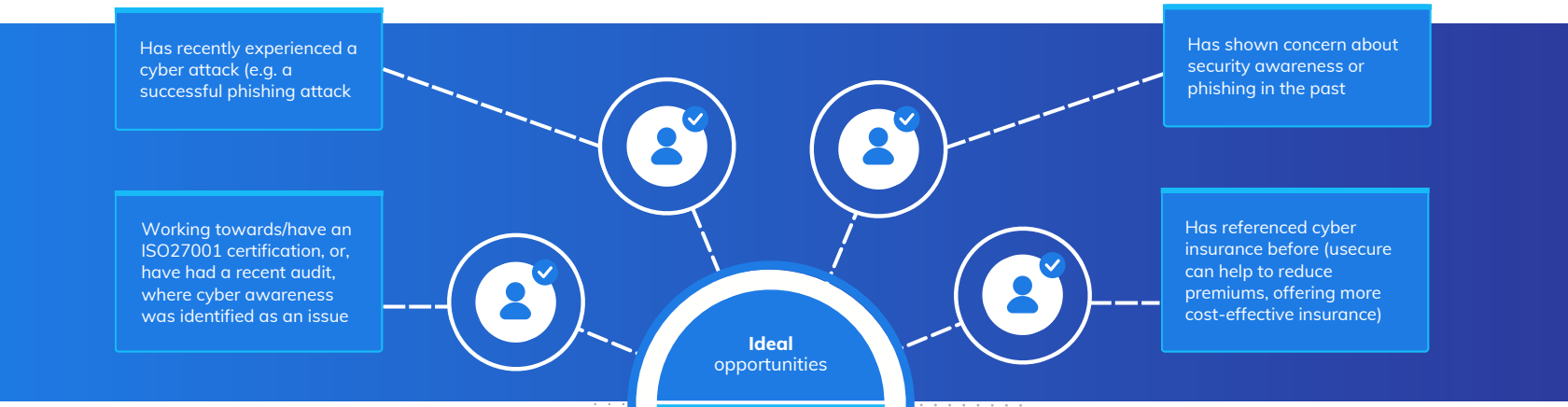
Boosting your service value

Bundling usecure alongside your existing products is a great way of increasing your service value and differentiating your offering in a crowded MSP market, without adding tonnes of manual work or complex pricing.

Here's an example of how to bundle usecure's suggested core and advanced plans:

Avoid itemising - We don't recommend selling usecure's features individually, as the product stack as whole is easier to sell and manage.

Identifying the ideal customer



Sales call script

Learn how best to respond in these common scenarios with a sales prospect.

MSP Intro

"Hi [Prospect], this is [Rep.Name] calling from [MSP]. We work with a specialist Human Risk Management company to raise end-user awareness of cyber security threats. Does Information Security fall under your responsibility at [Company]?"

Prospect Response

"Yes, that's my responsibility"

MSP Response

"Okay great, and what do you currently push out to your staff around security awareness training and phishing?"

"We don't push anything out currently"

MSP response - **Sell the requirement**

Find out why they're not currently pushing anything out: "No problem, is there any particular reason why you don't do anything around this? How do you ensure your staff are secure against things like phishing attacks?..."

View Full Script

"We do this ourselves / We're covered"

MSP response - **Uncover existing pain points**

Find out how they deliver training, who creates it, how long it takes to create and complete, and how do they track it. **If they already have a provider, go to** response three. If they do it themselves, say this: "We're finding a lot of those in infosec are spending a lot of time creating and delivering training in-house. We specialise in this area with 36 dedicated modules, and with our automated platform..."

View Full Script

"We already have a provider"

MSP response - **Find out renewal date + vendor info**

Find out who they're using, their experience with the provider and when the renewal is due. If their renewal is more than three months away, offer to send an email across and to get back in touch again 2-3 months before the renewal date. If the renewal is within the next three months, try to book in a 30-minute demo: "It's great that you take security awareness seriously, and with your renewal coming up soon it's always beneficial to spend 30 minutes taking a look at alternatives..."

View Full Script

Six common objections

"We haven't set aside a budget for this kind of thing"

Counter with:

- Turnkey: Full suite of services
- Cost of a breach is a lot higher
- Flexible monthly billing, per user
- Only pay for your monthly usage
- No long-term commitments

"It'll never happen to us, we wouldn't be targeted"

Counter with:

- 61% of SMBs have reported a cyber attack in the previous year
- Most attacks aren't targeted
- This is a good opportunity to offer a free Human Risk Report to demonstrate their vulnerability

"Sounds like a lot of new complicated processes"

Counter with:

- Automation: AutoEnrol manages each users' training for you
- No installations: 100% cloud-based
- Readily-made essential policies and phishing simulation templates
- Handheld onboarding by the MSP

"We already run training in-house now and then"

Counter with:

- Ask them what the training involves. Often, in-house training is irregular, doesn't cover essential topics, and is 'one-size-fits-all'.
- Once you've learned their approach, mention usecure differentiators.

"We don't have time to chase staff to complete courses"

Counter with:

- Automation: AutoEnrol sends automatic course reminders to users
- Staff can view their progress and activity inside their End User Portal
- Courses take 5-10 mins to complete and can be started when convenient.

"We ran this at my old company, it didn't work"

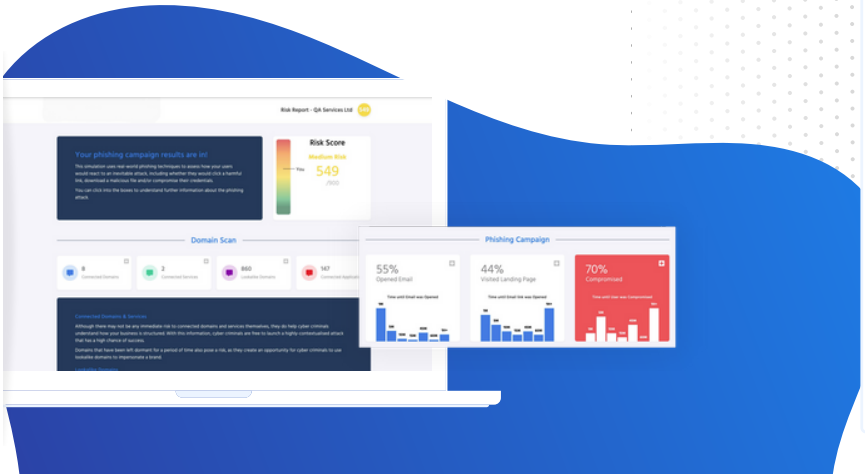
Counter with:

- Refer to usecure's key differentiators in this playbook to show how the service works compared others
- Make sure to position usecure as a human risk management solution.
- Share this brandable case study.

Sell faster with free Human Risk Reports

With the HRR prospecting tool, MSPs can calculate the employee cyber risk of new and prospective clients for free and in just a few clicks, then showcase this data to decision-makers to help:

- Generate more sales opps
- Win new clients faster
- Differentiate your service offering
- Unlock a gateway for selling other services



When to offer a HRR VS a free trial

HRR

The client needs convincing of the extent of the problem in their company. They need existing risk data to justify that this is a gap in their organisation. These prospects are usually earlier in the buying process as the project typically isn't something that's been approved.

Free Trial

The prospect knows they should implement a solution, but wants to take a closer look at the training / phishing templates to ensure this is the right solution for them.

OR

Training is their main driver and they just need to assess usecure's training content.

Learn more about HRR →

View Example Report →

How to get the most from the HRR

Setting clear expectations with clients *before* running a HRR is the key to selling usecure faster. Rather than selling these reports as a quick 'freebie', here's how to unlock their potential:

Get an upfront contract

Doing this before running a HRR helps identify more worthwhile prospects who want to justify a purchase. *"If we do find a lot of risk data, such as staff giving away a password during a phishing simulation, which actions would you want to take to mitigate those risks?"*. You can then refer to this post-HRR.

Set expectations

Ask the prospect their expectations for each stage (especially the breach scan and phish). If they're unsure, use examples of other companies, e.g. there will often be at least one user who's had their password breached, and at least one person who compromises to the phish (if they set up the spearphish).

Agree a timeframe

Agree a timeframe for running the HRR, including when allowlisting can be done. Don't let it drag. Emphasise how easy it is to start gathering data and setting up a phish.

Use a targeted phish

uPhish comes pre-loaded with both templated and spearphishing campaigns. To accurately gauge human risk to real-world attacks, we recommend suggesting the 'Holiday Policy' campaign, as this is a highly effective phish that's replicates a real-life attack.

Set up a follow-up call

Make sure to schedule a call for after the HRR is completed to discuss the risk results. Some MSPs have success when running a short call after the breach scan stage in order to review the data and confirm specifics on the phish. Some prospects, however, might just prefer having the pre-HRR and post-HRR calls.

Be transactional

In the post-HRR call, refer back to their expectations and upfront contract, e.g. "You mentioned that, if there's a staff compromise, you would want to roll out training and regular phishes. We can get a programme set up for you today for just £X per user, per month. Shall we get the training deployed today...?".

The road to recurring revenue

If a client runs a HRR, there should be enough risk data to justify a sale. Try to avoid running a follow-up free trial and, instead, be transactional.

Prospecting	Discovery Call	Human Risk Report		Free Trial	Convert to Paid
1	2	3	OR	3	4
Goal	**Goal**	**Goal**		**Goal**	**Goal**
Set discovery meeting	Start HRR/trial	Demonstrate risk		Demonstrate value	Start automatic billing
Actions	**Actions**	**Actions**		**Actions**	**Actions**
• Promote the service through calls, emails, social, etc. Register the discovery meeting.	• Run discovery meeting, qualify lead, identify pains, demo the service, promote the HRR/trial.	• Enrol client on a HRR. generate the report, and present the results in a follow-up meeting.		• Enable a free 14-day trial, help them enrol their users. book in a post-trial follow-up call.	• Run follow-up call, discuss how investing in training now will reduce their existing risk.
Tip	**Tip**	**Tip**		**Tip**	**Tip**
• Use the assets in usecure's Resource Hub, or, request a free branded pack from an Account Manager.	• Use the pointers in this partner playbook to help handle objections, convey the value and promote the HRR/trial.	• Explore a collection of HRR articles, demos and FAQs in the usecure Help Centre.		• Promote the free trial as an opportunity to run a gap analysis that shows where training is urgently needed.	• Upgrade the prospect to a paid account from their HRR summary or in the customer settings.

Partner Resource Hub

Marketing Hub

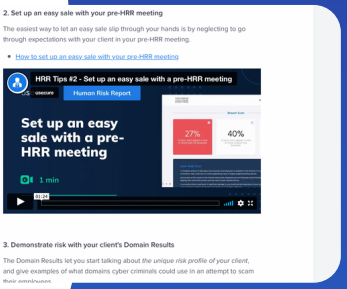
Access a library of white-labelled product sheets, case studies, eBooks, social media assets, landing page templates and more, to help you generate leads.

Go to Marketing Hub →

Sales Hub

Explore step-by-step resources that help you convert your usecure leads into paid clients, including a sales checklist, call scripts and tips for driving long-term revenue.

Go to Sales Hub →



Request a branded marketing bundle [free]

We want to help our partners hit the ground running. As a usecure partner, you can request a free marketing pack with your own branding — including videos, product sheets and more.

Request Free Bundle →

usecure