usecure

Selling and Scaling Human Risk Management

An MSP’s step-by-step guide to selling, packaging, and scaling Human Risk Management (HRM).

Table of contents

Introduction

A human risk management playbook

Traditional security awareness training falls short of today's cybersecurity demands. This playbook shares usecure's proven approach to help MSPs shift to full Human Risk Management (HRM) solutions that drive real results.

Based on our top-performing MSP partners, this guide helps you:

- Turn technical metrics into business value
- Position HRM as a strategic investment
- Overcome objections with tested tools
- Unlock recurring revenue through smart bundling

Get actionable insights, proven templates, and real-world examples to grow your security practice and better protect your clients.

> The biggest cybersecurity risk is people, not technology. Traditional training fails to change behavior, so MSPs must move beyond security awareness training to Human Risk Management.
>
> Embedding HRM boosts security, unlocks revenue, and strengthens client retention. This playbook guides you to real security outcomes and long-term growth.

Charles Preston
Founder and CEO, usecure

The MSP opportunity

Internal threats are driving demand for security awareness tools, with the market set to hit

$10B

by 2027 and MSP services topping $1T by 2033.

As security priorities shift, MSPs have a key opportunity to lead with solutions like usecure's HRM.

In this playbook, you'll find:

Plays
Leverage proven templates, scripts, and workflows to engage prospects at every stage of the sales journey—from initial outreach to closing the deal.

Tactics
Customize sales strategies with actionable tools like competitive battlecards, objection-handling scripts, and prospecting guides to address client pain points effectively.

Strategies
Align day-to-day sales actions with broader goals by positioning HRM as a proactive security investment that delivers measurable ROI and strengthens client relationships.

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

Get started with the usecure platform in just 15 minutes!

MSPs often face time constraints and technical challenges when deploying new solutions across diverse client environments.

Trigger

- Onboarding new clients.
- Addressing gaps in existing cybersecurity strategies.
- Clients requesting solutions beyond basic training programs.

Action

Deploy usecure quickly with these fast-start configurations:

1. Microsoft 365 Integration: Automate user synchronization with step-by-step guidance from our Microsoft 365 Synchronization guide.
   - Using Google Workspace? Follow our Google Workspace integration guide.

2. Automate Training (Auto-Enroll) – Seamlessly enroll users into security awareness training based on risk level or job role. Learn about Auto-Enroll.

3. **Automate Phishing (Auto-Phish)** – Launch simulated phishing campaigns automatically to test and improve user resilience. Get started with Auto-Phish

Download the Fast-Deployment Guide

usecure

Quick Start Deployment Guide

Get started with the usecure platform in just 15 minutes!

1 **Add administrators**
Invite team members to manage the platform. Add as many administrators as needed to ensure smooth access for all relevant personnel.

2 **Configure platform settings**
Customize the platform to meet your needs, including uploading your branding to course materials and emails. Review these settings before importing users.

3 **Import Users**
Easily import users using a CSV file or Microsoft 365 sync. Find more details in the article below.

4 **Add Managers**
Assign managers to oversee course participation and reporting for specific user groups.

5 **Ensure Email & Phishing Delivery**
Allow-list usecure IPs to ensure course emails and phishing simulations are delivered to users. Set up Message Injection for phishing emails.
- Microsoft 365: Allow-list IPs & set up Message Injection
- Google Workspace: Allow-list IPs & set up Message Injection
- Other Systems: Allow-list usecure IPs and domains

6 **Enrol Users**
Manually or automatically enrol users into security training. Let auto-enrolment take care of course assignments for you.

7 **Set Up Phishing Simulations**
Launch your first phishing simulation. Use auto-phish for automatic simulations or create custom ones.

👉 **Need step-by-step guidance?** Get started here for detailed setup instructions.

Users Love Us
High Performer Canada WINTER 2025
High Performer Small Business WINTER 2025
High Performer Mid-Market WINTER 2025

www.usecure.io |

Before we go any further... let's make deployment effortless

We get it. Even though usecure is quick to deploy, if your team hasn't set it up before (or in a while), it's easy to assume it'll take ages. The result? Clients are paying for usecure as part of their package, but it's not getting set up.

So, let's remove any barriers right now:

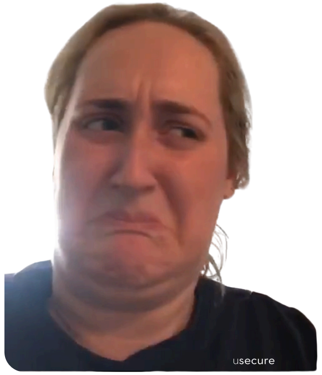
1. Fill out the quick form below about your typical client setup.

2. We'll generate a custom deployment guide with step-by-step instructions and screenshots.

3. Your tech team gets a ready-to-go reference for smooth, repeatable deployments.

No delays. No second-guessing. Just an easy, structured setup every time.

Get Started Now



Without guide

With a guide

Market trends driving HRM adoption

AI threats require adaptive learning solutions like usecure's bite-sized training modules that evolve alongside emerging risks.

Evolving cyber threats

AI-driven phishing campaigns and advanced social engineering tactics have made human vulnerabilities a primary target. In 2024, 90% of cyberattacks involved social engineering, with phishing as the most common method (Verizon DBIR 2024).

Remote work and shadow IT

The rise of remote work has increased reliance on unauthorized shadow IT tools, creating security blind spots. 68% of employees use unsanctioned apps, exposing organizations to compliance and data security risks (Gartner, 2024).

Human error

Infosec Institute reports that 74% of cybersecurity incidents include a human element. This includes falling for phishing attacks, sharing credentials, or mishandling sensitive data (IBM Cyber Security Intelligence Index Report).

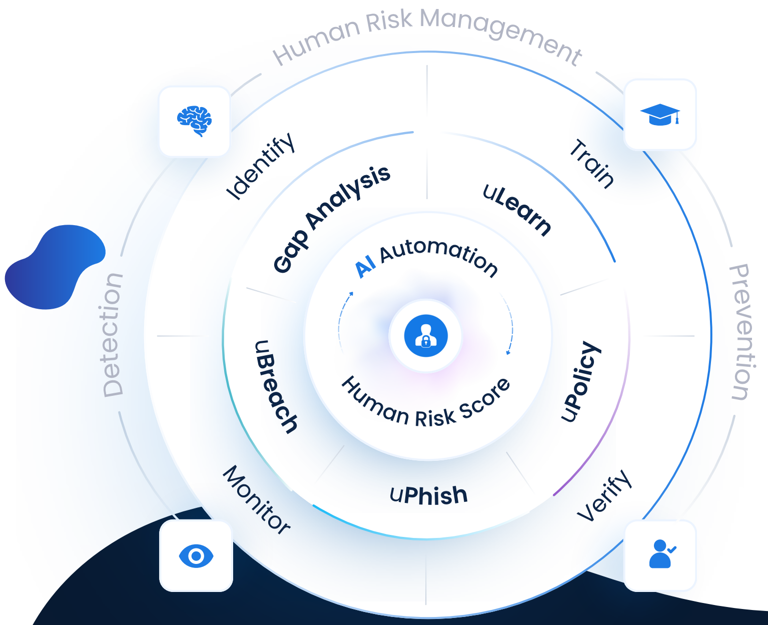
Compliance and cyber insurance

Stricter regulations like GDPR and ISO 27001 require robust risk management strategies. Additionally, cyber insurance premiums are projected to increase by 15% to 20% annually, reaching approximately $23 billion by 2026, up from an estimated $14 billion at the close of 2023. Insurers are increasingly demanding evidence of employee training and compliance measures.

How should MSPs position human risk management?

Human Risk Management (HRM) reduces human security risks by identifying vulnerable users, delivering targeted training, and tracking progress.

It’s a measurable, strategic solution MSPs can offer to boost security, support compliance, and show real value.



Identify

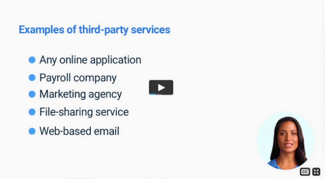
Spot key indicators or attributes that could leave users vulnerable, and determine likelihood of attack.

01

Train

Deliver targeted training based on observed areas of weakness, identified areas of risk.

02



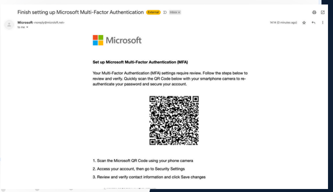
Examples of third-party services

- Any online application
- Payroll company
- Marketing agency
- File-sharing service
- Web-based email

Verify

Assess the impact of training through simulations that validate the effectiveness on user diligence of best practices.

03



Finish setting up Microsoft Multi-Factor Authentication External Inbox ×

Microsoft <noreply@microloft.net>
to me

14:14 (0 minutes ago)

Microsoft

Set up Microsoft Multi-Factor Authentication (MFA)

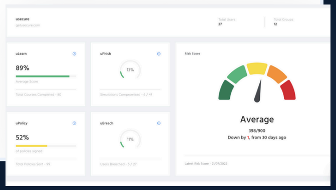
Your Multi-Factor Authentication (MFA) settings require review. Follow the steps below to review and verify. Quickly scan the QR Code below with your smartphone camera to re-authenticate your password and secure your account.

1. Scan the Microsoft QR Code using your phone camera
2. Access your account, then go to Security Settings
3. Review and verify contact information and click Save changes

Monitor

Source-based and behavioural analytics that continually monitors user performance and tracks increases or reductions in risk.

04



usecure
getusecure.com

Total Users 27
Total Groups 12

uLearn
89%
Average Score
Total Courses Completed - 80

uPhish
13%
Simulations Compromised - 6 / 44

uPolicy
52%
of policies signed
Total Policies Sent - 99

uBreach
11%
Users Breached - 3 / 27

Risk Score
Average
398/900
Down by 1, from 30 days ago
Latest Risk Score - 21/07/2022

Core usecure features to remember

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

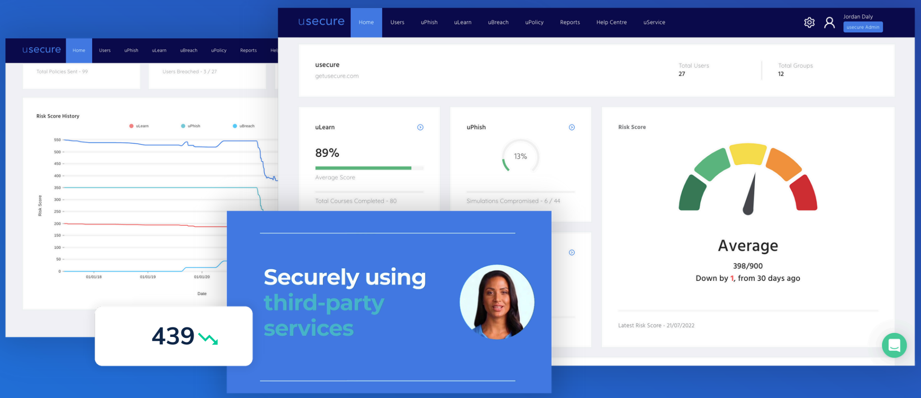
Policy management

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

Risk Reporting

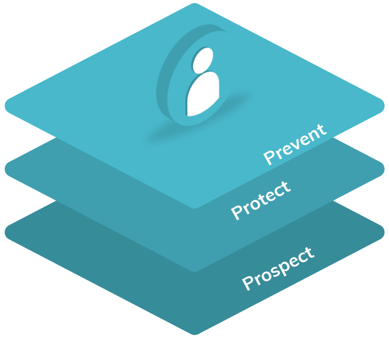
Human Risk Analytics

- 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



Feature upgrade: uBreach Pro

With uBreach Pro, MSPs can upgrade from usecure's standard dark web monitoring service, uBreach Starter, enabling partners to **enhance their security offering and unlock additional revenue through a premium add-on.**



Why uBreach Pro?

Elevate client security

Ensure your clients are always one step ahead of dark web threats.

Win new customers

Unlock a powerful sales tool that helps you sell your security services.

Enhance service value

Boost service value with a unique offering that instantly delivers value.

Learn More

- ✓ **Run free domain scans for prospects** and demonstrate the need for your service.
- ✓ **Protect in real-time with instant breach alerts** for your admins, clients and users
- ✓ **Monitor all emails under a given domain** to assess company-wide breaches.
- ✓ **Broaden your scope by monitoring** a greater number of data breach sources.

How MSPs drive additional recurring revenue with uBreach Pro

Available in several affordable and flexible domain usage packages, uBreach Pro comes as an additional charge on top of the core usecure platform. The monthly bill for partners reflects the volume of domains under monitoring.

Domain Usage Tiers

1-10	11-25	26-50	51-250	251-500	501+

Many usecure partners apply a fixed price per domain for their clients, enabling MSPs to achieve substantial ROI from the domains they purchase.

To obtain up-to-date pricing for each tier, reach out to your usecure Account Manager or chat with our team via our live chat.

How to package usecure

We recommend splitting your subscription options into two tiers - Core and Advanced. This helps keep your clients' options flexible, while 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
	uBreach Automated breach scans
	Reporting Automated reporting
		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
			£1.50–£2
			per user/ per month
			USD = $2.00
			AUD = $3.00
			EUR = €1.85
			NZD = $3.50
			ZAR = R35.00

Advanced
Enhance value and grow your margins, whilst keeping admin low
	Custom phishing campaigns
	Custom user training courses
	uPolicy Policy management and tracking
	uBreach Pro Advanced dark web monitoring +
		Admin Time = Low
		Readily-made phishing and policy templates
		Easily build custom courses
		Distribute your custom content amongst other clients to save time
			£2.50–£3
			per user/ per month
			USD = $3.20
			AUD = $5.00
			EUR = €3.00
			NZD = $5.50
			ZAR = R57.00

✓ 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.

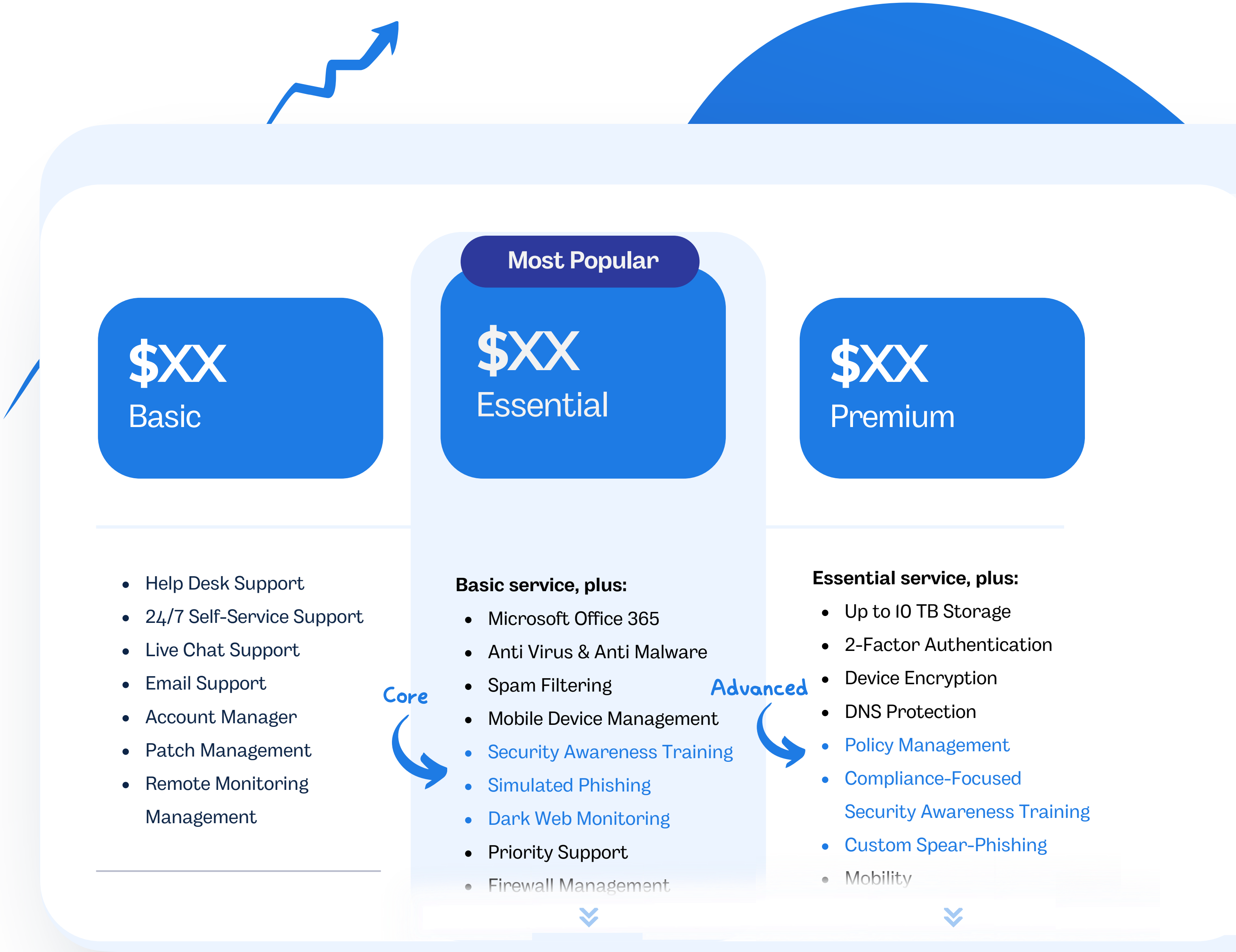
Growth tip: Enhance your margins with uBreach Pro

MSPs can price uBreach Pro **per domain** (e.g., £40/$50) or bundle it in an '**Advanced**' subscription to boost margins and RRP as a premium offering. Learn more on page 13.

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:



$XX
Basic

- Help Desk Support
- 24/7 Self-Service Support
- Live Chat Support
- Email Support
- Account Manager
- Patch Management
- Remote Monitoring Management

Most Popular

$XX
Essential

Basic service, plus:

- Microsoft Office 365
- Anti Virus & Anti Malware
- Spam Filtering
- Mobile Device Management
- Security Awareness Training
- Simulated Phishing
- Dark Web Monitoring
- Priority Support
- Firewall Management

$XX
Premium

Essential service, plus:

- Up to 10 TB Storage
- 2-Factor Authentication
- Device Encryption
- DNS Protection
- Policy Management
- Compliance-Focused Security Awareness Training
- Custom Spear-Phishing
- Mobility

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

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

Who are you selling to?

Before diving into how to package and sell usecure effectively, it's important to understand the key buyer personas MSPs typically encounter. Each persona has unique pain points, priorities, and decision-making criteria. Tailoring your pitch to these personas will help you close deals faster and build stronger client relationships.

IT Managers at SMBs

Challenge

- Overwhelmed by managing IT infrastructure with limited resources.
- Struggle to ensure employees follow security protocols.

Need

- Automated solutions that reduce manual effort and improve security outcomes.
- Tools that simplify compliance audits and reporting.

Business Owners / Executives

Challenge

- Concerned about financial loss or reputational damage from cyber incidents.
- Increasing pressure to meet cyber insurance or compliance requirements.

Need

- Clear ROI and measurable risk reduction to justify investment.
- Proactive solutions that protect their business without disrupting operations.

HR or Compliance Officers

Challenge

- Difficulty engaging employees in training programs.
- Struggle to track policy acknowledgments and ensure audit readiness.

Need

- User-friendly platforms that drive employee participation and simplify compliance.
- Automated tools for policy management and reporting.

How these personas align with packaging plans

- **Core Plan**: Ideal for IT Managers who need a quick, automated solution to improve employee awareness without adding complexity.
- **Advanced Plan**: Perfect for Business Owners or Compliance Officers who require tailored solutions with advanced features like policy management or custom phishing templates.

How to pitch HRM to different buyer personas

Before pitching usecure effectively, MSPs must tailor their approach based on the prospect's role, challenges, and priorities. Below is a structured guide on how to communicate HRM's value to different decision-makers.

Persona	Pain Points	How to Position HRM	Key Messaging Tips
IT Managers at SMBs	• Limited time/resources - Struggle with user compliance • Need automation & visibility	• Make their job easier with automation • Reduce workload with seamless integrations (Microsoft 365, Google Workspace) • Improve compliance without manual intervention	• "HRM automates training, policies, and reporting so you don't have to manually chase employees or track progress." • "You'll have a dashboard to see which employees pose the biggest security risks—without running manual audits."
Business Owners / Executives	• Financial risk from cyber incidents • Cyber insurance & compliance pressures • Worried about reputational damage	• Risk-based approach: usecure reduces liability and ensures regulatory compliance • Competitive advantage: A secure company builds customer trust	• "90% of breaches come from human error—HRM actively reduces risk, not just reports on it." • "Clients that prioritize HRM have lower insurance premiums and fewer security incidents."
HR / Compliance Officers	• Ensuring employees complete training • Tracking policy compliance • Audit readiness & reporting headaches	• Automated compliance management saves time • Instant reporting for audits & insurance • Better employee engagement with shorter, interactive training	• "Instead of chasing employees, HRM automates reminders and ensures full policy acknowledgment." • "You can instantly pull compliance reports for auditors—no more spreadsheets or manual tracking."

Before moving forward, make sure you've identified your ideal SMB clients. If you haven't, take a moment to define your target market using the buyer personas outlined above.

✓ Action Step: Review the Buyer Personas section and write down your top 3 target SMB types.

Dive into our Go-to Market HRM Strategy for in-depth steps >

Positioning: HRM vs. training-only solutions

> “If HRM is the clear solution, how do you position it to clients who are stuck in the ‘training-only’ mindset?”

Feature	Traditional SAT	Human Risk Management (HRM)
Training Approach	One-size-fits-all, periodic sessions	Adaptive, ongoing, bite-sized learning
Automation	Minimal	Fully automated training, policy enforcement, and risk scoring
User Risk Scoring	Not included	Tracks individual risk levels for targeted interventio
Policy Management	Manual, inconsistent	Automated distribution, tracking, and compliance auditing
Threat Readiness	Limited to awareness	Actionable insights, real-world phishing simula and behavior analytics

☑ Automation:

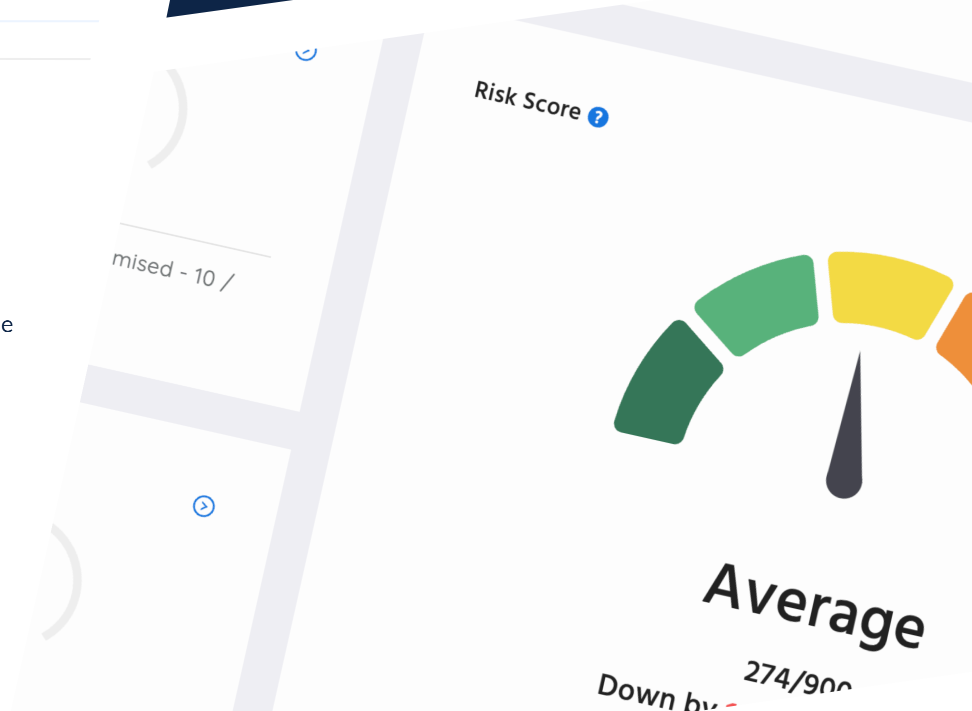
- Automated phishing simulations, training enrollment, and policy management save time for MSPs and reduce manual effort.
- Features like auto-enrollment ensure that users are seamlessly onboarded into tailored training programs based on their risk profiles.

☑ User Risk Scoring:

- Identify high-risk users through continuous monitoring and tailor interventions to mitigate vulnerabilities effectively.
- Provides actionable insights by quantifying individual user risk through metrics such as phishing simulation performance and dark web exposure.

☑ Policy Management:

- Simplifies compliance by automating the creation, distribution, and tracking of security policies.
- Ensures employees stay informed about security standards while making audits easie clients.



The competition

View G2's latest competitor analysis

Latest Comparison

Independent reviews sourced from G2's Grid® Report for Security Awareness Training | Spring 2025

	usecure	KnowBe4	MetaCompliance
Meets requirements	93%	94%	91%
Ease of setup	93%	90%	89%
Ease of use	93%	92%	89%
Customization	88%	86%	85%
Phishing assessment	94%	94%	91%
Quality of support	95%	94%	96%
Risk scoring	97%	84%	84%
Continuous assessment	93%	90%	Feature rating unavailable
Reporting	88%	Feature rating unavailable	Feature rating unavailable

Six common objections

"We already have a cybersecurity solution in place."

Counter with:

- Layered security approach: Technical defenses don't address human risk—90% of breaches involve human error.
- Complement, not replace: usecure strengthens existing security by reducing risky behaviors.

"We don't see enough value to justify the cost.."

Counter with:

- Cost of inaction: A single breach costs significantly more than proactive risk management.
- Clear ROI: Fewer incidents, lower cyber insurance premiums, and stronger compliance.

"We're too small for this."

Counter with:

- SMBs are prime targets: Hackers know smaller businesses lack dedicated security teams.
- Affordable & scalable: Tailored pricing ensures it fits businesses of all sizes.

"My staff members won't actually engage with a programme?"

Counter with:

- MSP-exclusive benefits: Additional management, support, and strategic guidance that vendors don't offer.
- Fully managed service: Saves their internal team time while ensuring proper implementation.

"We've never had a security incident, so we don't need this."

Counter with:

- Security isn't about luck: Breaches happen without warning—prevention is cheaper than response.
- Compliance & insurance: Proactive HRM helps meet evolving security requirements.

"We tried this before, and it didn't work."

Counter with:

- What didn't work? Identify past issues and highlight how usecure solves them.
- Proven engagement: Personalized, bite-sized training drives better results.

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

How to sell HRM as a strategic security investment

> HRM is a strategic security layer that complements existing technical defenses like firewalls.
>
> By reducing human risk, HRM enhances an organization’s resilience to threats and fosters a security-conscious workforce.

The Human Side of Risk Management

HRM places people at the center of security. It recognizes that human behavior—the decisions, mistakes, and instincts of employees—is a critical factor in cybersecurity. Just as we assess personal risks in daily life, businesses must understand and manage the human element of organizational risk.

Human-Centered Risk Management: A Strategic Shift

- **Identify and Address Human Risk**: HRM automatically flags high-risk behaviors and delivers targeted interventions.
- **Promote Continuous Learning**: HRM ensures employees are consistently trained with adaptive, bite-sized content, evolving alongside emerging threats.
- **Foster Empathy and Responsibility**: By involving employees in security, HRM makes them an integral part of the solution.

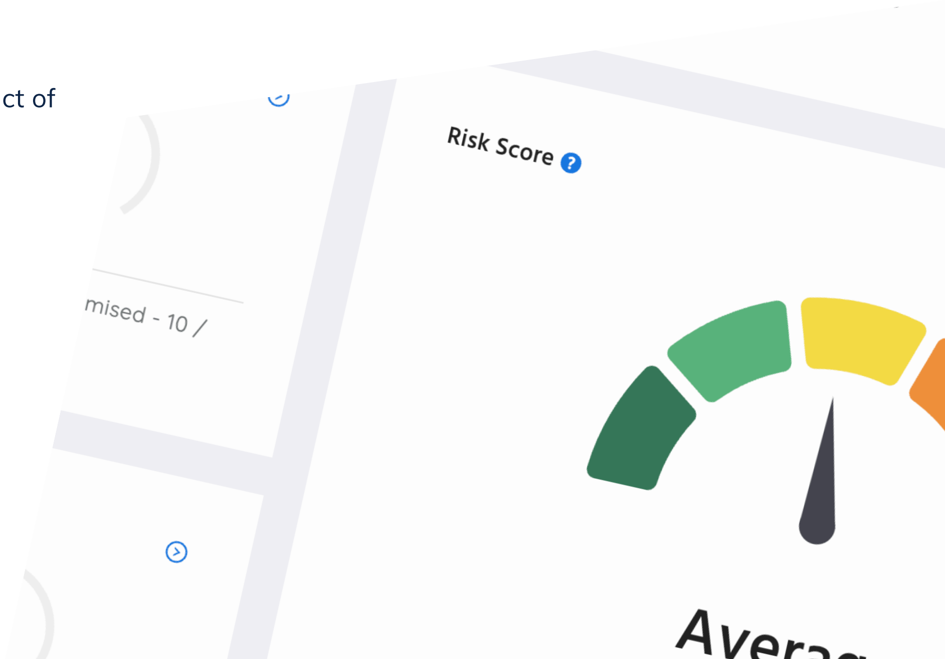
ROI Storytelling: Positioning HRM as a Strategic Investment

Instead of focusing on training completion rates, MSPs should talk about the real-world impact of HRM—reduced risk and increased organizational resilience.
Here are ways to frame HRM’s ROI:

☑ Proactive Risk Reduction:
“Rather than simply completing training, HRM enables you to identify high-risk behaviors and target specific employees for tailored interventions. This leads to fewer security incidents.”

☑ Cost Avoidance:
“With HRM, your organization can avoid costly breaches, which average $4 million globally, by addressing human risk before it materializes.”

☑ Improved Compliance:
“HRM makes it easier to comply with regulations like GDPR and ISO 27001 by reducing human errors, streamlining compliance workflows, and providing automated reporting.”



Outreach: Connecting with the right prospects

Once we know who we want to sell to, it's time to reach out. A well-structured outreach strategy ensures you connect with the right prospects at the right time, increasing your chances of closing deals.

Example Sales Pitches

Email Pitch

Subject Line: Reduce Your Cyber Risk with One Simple Step
Hi [First Name],

I noticed that [Company Name] operates in [Industry], where phishing and compliance risks are growing concerns.

We specialize in helping businesses like yours reduce human cyber risk through automated training, phishing simulations, and policy management.

Would you be open to a quick call? I'd love to share how our platform has helped businesses like [Case Study Example] reduce phishing risk by 90%.

Best regards,
[Your Name]

Phone Script
"Hi [Prospect], this is [Your Name] from [Your MSP]. We help businesses reduce human cyber risk through proactive solutions that go beyond traditional training programs.

I'd love to schedule a quick call to show you how we've helped companies like yours improve security awareness while simplifying compliance."

> The key is to use a routine cadence—a combination of outreach tactics repeated systematically for each prospect. This approach ensures consistent follow-ups and keeps your message in front of potential buyers.

Nihil Morjaria
Chief Revenue Officer
at usecure

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 you checking our comprehensive template library available via your partner portal.

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 human-centered approach to compliance & cyber insurance

HRM isn't just another security tool—it's a growth opportunity for MSPs. By addressing the human element of cybersecurity, MSPs can strengthen client relationships, increase retention, and create new revenue streams through automation and advanced services.

Why Compliance & Cyber Insurance Require a Human Risk Strategy:

- Regulatory mandates (GDPR, HIPAA, ISO 27001) require organizations to manage human risk, making HRM essential for audits & liability reduction.
- Cyber insurers increasingly demand proactive security measures—lack of compliance can lead to denied claims or higher premiums.
- SMBs face growing pressure from partners & clients to demonstrate cybersecurity resilience.

How HRM Simplifies Compliance & Reduces Liability Risks

✅ Automated Policy Management – Ensures security standards are met with audit-ready documentation.
✅ Risk-Based Training & Reporting – Tailored programs address compliance needs while automated reports simplify audits.
✅ Proactive Risk Mitigation – Features like phishing simulations & dark web monitoring prevent threats before they escalate.

Selling HRM Through Compliance & Insurance Trends

- Educate Prospects – Show financial & reputational risks of non-compliance.
- Demonstrate Value – Use Human Risk Reports (HRR) to highlight vulnerabilities.
- Position HRM as a Dual Solution – Compliance enabler & risk mitigator.
- Leverage ROI Storytelling – Show real-world success in reducing audit times, preventing fines & lowering premiums.

Sales Enablement Resources for MSPs

Email Templates – Industry-specific messaging linking compliance challenges to HRM benefits. Download Email Templates.

Pitch Deck – Visual storytelling on HRM's role in risk reduction & compliance readiness. Download Pitch Deck.

By prioritizing the human element in risk management, MSPs can strengthen client security, streamline compliance, and unlock new revenue opportunities.

How HRM increases client retention & upsell revenue

HRM isn't just another security tool—it's a growth opportunity for MSPs. By addressing the human element of cybersecurity, MSPs can strengthen client relationships, increase retention, and create new revenue streams through automation and advanced services.

Case Study: IT Visionaren

- Challenge: IT Visionaren needed to train hundreds of end users across multiple clients without overwhelming their small team with administrative tasks.
- Solution: By leveraging usecure's AutoEnrol and AutoPhish features, IT Visionaren automated training enrollment and phishing simulations, reducing manual effort while improving client security awareness.
- Result: Clients reported increased employee awareness of cyber threats, particularly phishing attacks, while IT Visionaren scaled their services with minimal admin overhead.
- Key Takeaway: Automation allowed IT Visionaren to protect client environments efficiently while focusing on business growth.

Aspect	Traditional SAT	Human Risk Management
Focus	Training completion rates	Risk reduction and behavior change
Engagement	Generic, one-size-fits-all	Personalized, bite-sized training
Impact	Limited measurable outcomes	Reduced phishing susceptibility, improved compliance readiness
Scalability	Manual processes per client	Automated enrollment, training, and reporting

HRM's Impact on Client Retention & Revenue

- **Higher Retention**: Clients renew when they see measurable security improvements, like reduced phishing risks and faster compliance.
- **Upsell Potential**: Bundle HRM with premium add-ons like dark web monitoring or advanced reporting to increase contract value.
- **Scalable Growth**: Automation minimizes admin work, allowing MSPs to expand services without adding resource costs.

How MSPs Can Maximize HRM for Growth

- **Prove Value with Data**: Show reduced risk scores and phishing resilience to build trust.
- **Position HRM as Essential**: Present it as a proactive security layer alongside technical defences.
- **Bundle for More Revenue**: Package HRM with email security or MFA for comprehensive protection.

Download Case Studies

Follow up templates

Post-Discovery Call Follow-Up

Subject Line: Next Steps: Reducing Human Risk at [Client Name]

Hi [First Name],

Thank you for taking the time to discuss your cybersecurity needs today! As mentioned, we'd love to run a quick Human Risk Report for your team to identify specific vulnerabilities and provide actionable insights on reducing risk.

Let me know a good time next week for us to get started!
Best regards,

[Your Name]

Post-Trial Follow-Up

Subject Line: Results from Your Free Trial with [Your MSP]

Hi [First Name],

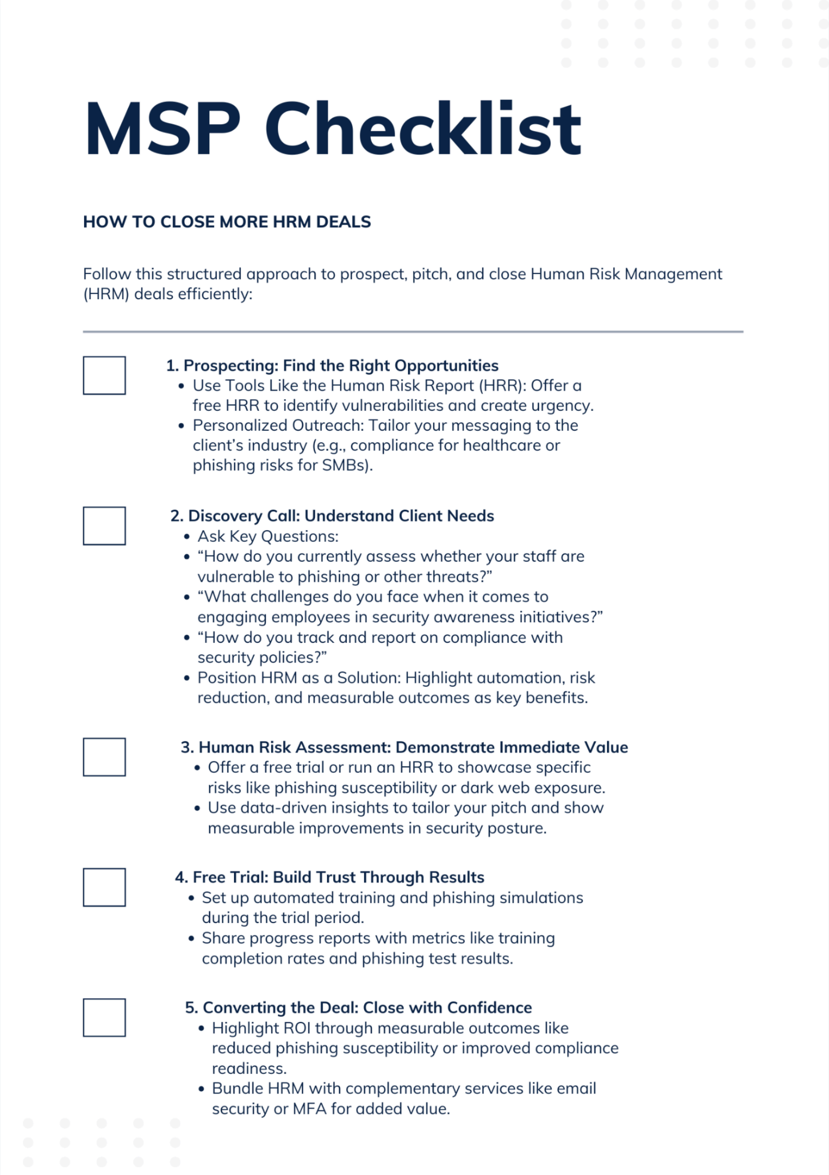
I hope you've had a chance to review the results from your free trial! Here's what we've achieved so far:

- [Metric 1: e.g., % of employees completing training.]
- [Metric 2: e.g., % of phishing simulations successfully identified.]

Based on these results, we'd love to discuss how we can continue reducing human risk across your organization with our full solution.

Let me know when you're available for a quick call!

Best regards,
[Your Name]



MSP Checklist

HOW TO CLOSE MORE HRM DEALS

Follow this structured approach to prospect, pitch, and close Human Risk Management (HRM) deals efficiently:

□ **1. Prospecting: Find the Right Opportunities**
- Use Tools Like the Human Risk Report (HRR): Offer a free HRR to identify vulnerabilities and create urgency.
- Personalized Outreach: Tailor your messaging to the client's industry (e.g., compliance for healthcare or phishing risks for SMBs).

□ **2. Discovery Call: Understand Client Needs**
- Ask Key Questions:
- "How do you currently assess whether your staff are vulnerable to phishing or other threats?"
- "What challenges do you face when it comes to engaging employees in security awareness initiatives?"
- "How do you track and report on compliance with security policies?"
- Position HRM as a Solution: Highlight automation, risk reduction, and measurable outcomes as key benefits.

□ **3. Human Risk Assessment: Demonstrate Immediate Value**
- Offer a free trial or run an HRR to showcase specific risks like phishing susceptibility or dark web exposure.
- Use data-driven insights to tailor your pitch and show measurable improvements in security posture.

□ **4. Free Trial: Build Trust Through Results**
- Set up automated training and phishing simulations during the trial period.
- Share progress reports with metrics like training completion rates and phishing test results.

□ **5. Converting the Deal: Close with Confidence**
- Highlight ROI through measurable outcomes like reduced phishing susceptibility or improved compliance readiness.
- Bundle HRM with complementary services like email security or MFA for added value.

Download Checklist ⟶

Keys to MSP marketing & sales success

To wrap up, here are the three most important takeaways for MSPs selling HRM solutions.

1. Speak the Client's Language

Don't sell "security training"—sell risk reduction and compliance ease.

Example: Instead of "This solution includes phishing training," say, "This solution helps you stop staff from clicking phishing emails in the first place."

2. Make It Easy to Buy & Implement

Position HRM as a fully managed service so clients see it as a hands-off, high-value solution.

Example: "You don't have to do anything manually—our system automatically enrolls, trains, and reports compliance status for you."

3. Show Immediate Value

Use trials and reports to reveal risk exposure instead of just selling training.

Example: "Let's run a quick gap analysis—if you have employees failing phishing tests, we'll fix it before an actual attack happens."

Get Started Today

- **Step 1:** Identify your ideal prospects using the Prospecting Guide.
- **Step 2:** Use the Discovery Questions to uncover client pain points.
- **Step 3:** Offer a trial or risk report to show immediate value.
- **Step 4:** Close the deal using the objection-handling framework.

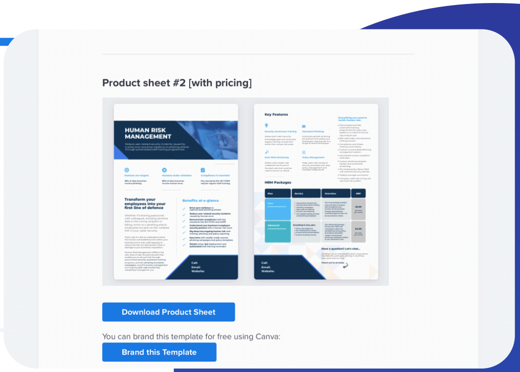
By following this playbook, MSPs can increase revenue, improve client security, and build stronger long-term relationships—positioning themselves as strategic cybersecurity leaders.

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 ⟶



Product sheet #2 [with pricing]

Download Product Sheet

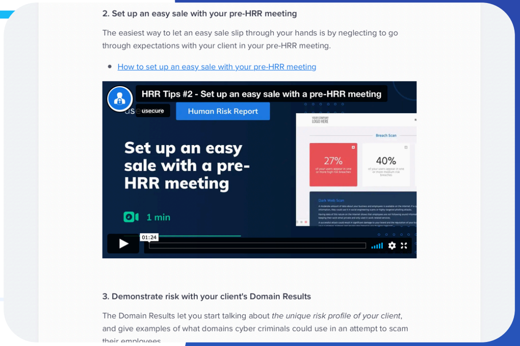
You can brand this template for free using Canva:

Brand this Template

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 ⟶



2. Set up an easy sale with your pre-HRR meeting

The easiest way to let an easy sale slip through your hands is by neglecting to go through expectations with your client in your pre-HRR meeting.

- How to set up an easy sale with your pre-HRR meeting

HRR Tips #2 - Set up an easy sale with a pre-HRR meeting
usecure
Human Risk Report
Set up an easy sale with a pre-HRR meeting
1 min
27%
40%
01:24

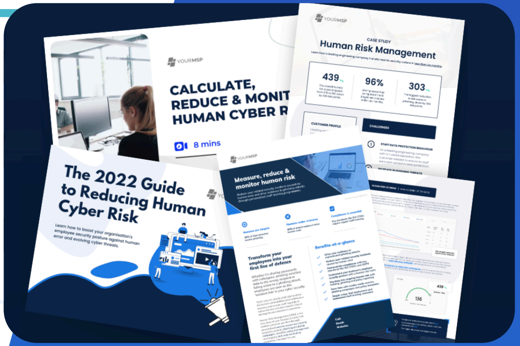
3. Demonstrate risk with your client's Domain Results

The Domain Results let you start talking about *the unique risk profile of your client*, and give examples of what domains cyber criminals could use in an attempt to scam their employees

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 ⟶



CALCULATE, REDUCE & MONIT
HUMAN CYBER R
8 mins
Human Risk Management
439
96%
303
The 2022 Guide to Reducing Human Cyber Risk
Measure, reduce & monitor human risk

usecure