

Human Risk Management(HRM)

PURCHASING TOOLKIT

A Strategic Framework for Evaluating and
Advancing Human Risk Governance



Living Security helps organizations measure and reduce human cyber risk through AI-native Human Risk Management (HRM). This strategic toolkit is designed to help security leaders understand the HRM model, assess current maturity, and define a path toward measurable risk governance.

How to Use This Toolkit

This guide is designed to help security leaders understand, evaluate, and operationalize Human Risk Management (HRM).

Inside this toolkit, you will:

- Understand why traditional awareness metrics fail to quantify exposure
- Learn the structural differences between SAT and AI-native HRM
- Assess your current maturity level
- Explore purchasing and deployment models
- Identify next steps for measurable risk reduction

This document is part of a broader HRM resource series:

- Executive Business Case Pack
- 90-Day HRM Deployment Playbook
- HRM RFP & Vendor Evaluation Kit

INTRODUCTION:

The Cost of Measuring the Wrong Things

In 2024, **74% of breaches involved a human element**¹, according to the Verizon Data Breach Investigations Report (DBIR). Yet most enterprises, including teams like yours, still measure human security risk with just two metrics: training completion rates and phishing click percentages.

That gap is becoming expensive.

The **average cost of a data breach now exceeds \$4.8 million**², and incidents involving human error, credential misuse, or social engineering often carry the highest remediation and recovery costs (IBM Cost of a Data Breach Report). If you can't identify your highest-risk users before an incident, you're paying for that visibility in incident response dollars.

Meanwhile, pressure is mounting:

- **Boards** are demanding measurable risk reduction, not activity reports.
- **Cyber insurers** are scrutinizing behavioral controls and identity protections.
- **Regulators** increasingly expect demonstrable, risk-based safeguards, not annual proof-of-training certificates.
- **AI-enabled attacks**, from deepfake impersonation to automated phishing at scale, are bypassing static, simulation-based awareness programs.

The threat environment has evolved. Human risk measurement has not.

¹ Human element in breaches statistic: Source: Verizon 2024 Data Breach Investigations Report (DBIR), 2024. Available at: <https://www.verizon.com/business/resources/reports/dbir/>

² Average cost of a data breach statistic: Source: IBM/Ponemon Institute Cost of a Data Breach Report 2025. Available at: <https://www.ibm.com/security/data-breach>

Completion rates and phishing simulations show participation. They do not quantify exposure. They do not identify which users pose disproportionate risk. And they do not reflect how modern threats unfold across identity systems, collaboration platforms, AI assistants, and cloud environments.

Security leaders are now confronting a more fundamental question:

Instead of asking,

"Did employees complete training?"

They are asking,

"Are we measurably reducing human-driven cyber risk across the enterprise?"

That shift, from activity tracking to risk governance, is redefining how organizations approach the human layer of cybersecurity.

In an era where both attackers and employees are augmented by AI, organizations can no longer rely on periodic awareness events to manage dynamic human risk. The companies that can quantify, prioritize, and continuously reduce human-driven exposure will be the ones that can confidently demonstrate security ROI to boards, insurers, and regulators alike.

If traditional awareness metrics cannot quantify exposure, identify high-risk users, or prioritize intervention, what does?

To reduce risk, **your team needs** a model that integrates behavioral signals, identity risk, technical telemetry, and real-world threat patterns into a unified picture, so you can act, not just report.

That model is Human Risk Management. The next section breaks down what it is, how it works, and why it represents a structural evolution beyond legacy SAT programs.

PROOF POINT:

"In 2024, 74% of breaches involved a human element, yet only about 10% of organizations have adopted progressive Human Risk Management capabilities, leaving most with limited visibility into human-driven risk."

Source: Verizon Data Breach Investigations Report 2024; Forrester Wave™ Human Risk Management, Q3 2024
<https://www.verizon.com/business/resources/reports/dbir/> | <https://www.livingsecurity.com/forrester-wave-report-2024>

THE BUSINESS PROBLEM:

Why Security Awareness Alone Fails to Reduce Risk

Most Security Awareness Training (SAT) programs were designed to satisfy compliance requirements. They typically consist of annual or periodic training, phishing simulations, and participation tracking.

While necessary, this model has structural limitations. It is:

- **Reactive** rather than continuous
- **One-size-fits-all** rather than risk-based
- **Isolated** from broader security telemetry
- **Measured by completion** rather than measurable impact

These limitations are not theoretical. They show up in breach reports. Consider a composite example drawn from real-world incident patterns:

An employee completes annual training and passes multiple phishing simulations. Their record shows low click rates and full compliance. From a SAT perspective, they are “low risk.”

Months later, attackers use AI-generated reconnaissance to craft a highly personalized message that does not resemble prior simulations. The employee’s credentials are harvested. Within hours, the attacker initiates unusual login patterns, downloads sensitive data, and moves laterally using privileged access.

The warning signs were present: anomalous identity activity, abnormal endpoint behavior, unusual data movement. But those signals were visible in identity and endpoint telemetry, not in phishing simulation dashboards.

The organization had training completion metrics. It did not have unified human risk visibility. This is the structural blind spot of traditional SAT.

Because SAT programs rely largely on simulated phishing and course participation, they typically monitor **5 to 10 phishing-related behaviors**. Modern Human Risk Management platforms, by contrast, can track **200+ discrete behavior and risk signals** across identity misuse, endpoint activity, access anomalies, AI tool usage, and data movement patterns.

That means traditional SAT captures **less than 5% of the behavioral signals** that indicate elevated human cyber risk in today's environments.

As threat sophistication increases, particularly through AI-enabled phishing, impersonation, behavioral mimicry, and automated attack chains, point-in-time awareness programs cannot keep pace. To keep pace with AI-enabled attacks, **you need** continuous visibility into human risk, and the ability to intervene dynamically.

The core issue isn't whether employees complete training. It's whether **you can** identify and reduce high-risk behavior before it becomes a breach.

This gap between simulated measurement and real-world exposure is what Human Risk Management is designed to close.



PROOF POINT:

"One vendor cited in Forrester's HRM Wave tracks only 13 cybersecurity behaviors—highlighting why phishing-centric measurement cannot represent enterprise-wide human risk."

Source: Forrester Wave™ Human Risk Management, Q3 2024 <https://www.livingsecurity.com/forrester-wave-report-2024>

FROM AWARENESS TO GOVERNANCE:

The HRM Operating Model

What Is Human Risk Management (HRM)?

Human Risk Management (HRM) is the evolution of traditional Security Awareness Training (SAT) into a measurable, intelligence-driven risk discipline.

HRM treats human behavior, and the AI systems acting on human intent, as a measurable, governable risk surface.

Unlike SAT, which focuses primarily on compliance-driven training and phishing simulations, HRM provides **continuous visibility into workforce risk across identity, access, activity, and exposure**, then applies targeted interventions to measurably reduce that risk over time.

With HRM, **you integrate** behavioral and technical signals from:

- Identity providers
- Email and collaboration platforms
- Endpoint and device telemetry
- Data Loss Prevention (DLP) systems
- Access and privilege management tools
- AI and agent usage environments

These signals are synthesized into dynamic risk scoring at the individual, team, and enterprise levels.

HRM transforms security training from a periodic, one-size-fits-all compliance exercise into a continuous, data-driven risk management discipline.

With HRM, **you can**:

- Quantify human risk across individuals, teams, and the enterprise
- Identify high-risk behaviors and concentrated risk cohorts
- Reduce **exposure duration** — the time users remain in elevated risk states
- Deliver personalized interventions and behavior scorecards
- Provide executive reporting tied to measurable risk movement

This shift from activity-based reporting (completion and click rates) to risk-based governance makes HRM board-relevant and strategically aligned.

SAT vs. HRM: Structural Comparison

Traditional SAT platforms typically monitor 5–10 phishing-related behaviors. Modern HRM platforms track 200+ discrete signals across identity misuse, access anomalies, endpoint behavior, AI usage, and data movement, expanding observable human risk visibility by 20x+ compared to phishing-only metrics.

The difference is structural, not incremental.

Feature/Capability	Traditional SAT	HRM-Integrated Approach
Training Delivery	Annual, generic	Continuous, personalized
Risk Detection	Manual, periodic	Automated, real-time
Data Integration	Siloed	Unified, cross-tool
Intervention Triggers	Manual, after incident	Automated, proactive
Reporting	Completion/click rates	Risk reduction, behavior change
Engagement	Passive, compliance	Gamified, positive reinforcement
Executive Visibility	Limited	Board-ready, actionable
Exposure Duration Tracking	No visibility into time-at-risk	Continuous measurement & reduction of elevated risk states

The Human Risk Management Maturity Model

Organizations typically progress through five distinct stages of human risk maturity across three core dimensions: Culture, Technology, and Process. This model helps security leaders assess their current state and plan the journey from compliance-driven awareness to predictive, AI-powered human risk management.

Stage	Strategic Theme	Culture	Technology	Process
Initial	Compliance	Compliance-driven engagement	LMS & phishing tools	Reactive, participation-based
Managed	Emerging Visibility	Role-based segmentation	Manual tracking	Limited risk-based intervention
Defined	Intelligence	Leadership alignment	Cross-tool integration	Risk movement measured
Optimized	Proactive Governance	Shared accountability	AI-assisted monitoring	Measurable exposure duration reduction
Innovating	Predictive	Workforce ownership	Predictive AI & dynamic controls	Real-time adaptive intervention

Where Is Your Organization Today?

Most teams recognize themselves somewhere between **Initial** and **Defined** maturity.

The critical question is not whether training exists. It is whether **you** have:

- Continuous visibility into human and agentic risk
- Clear measurement of exposure duration
- Automated, risk-based intervention workflows
- Executive reporting tied to measurable risk reduction

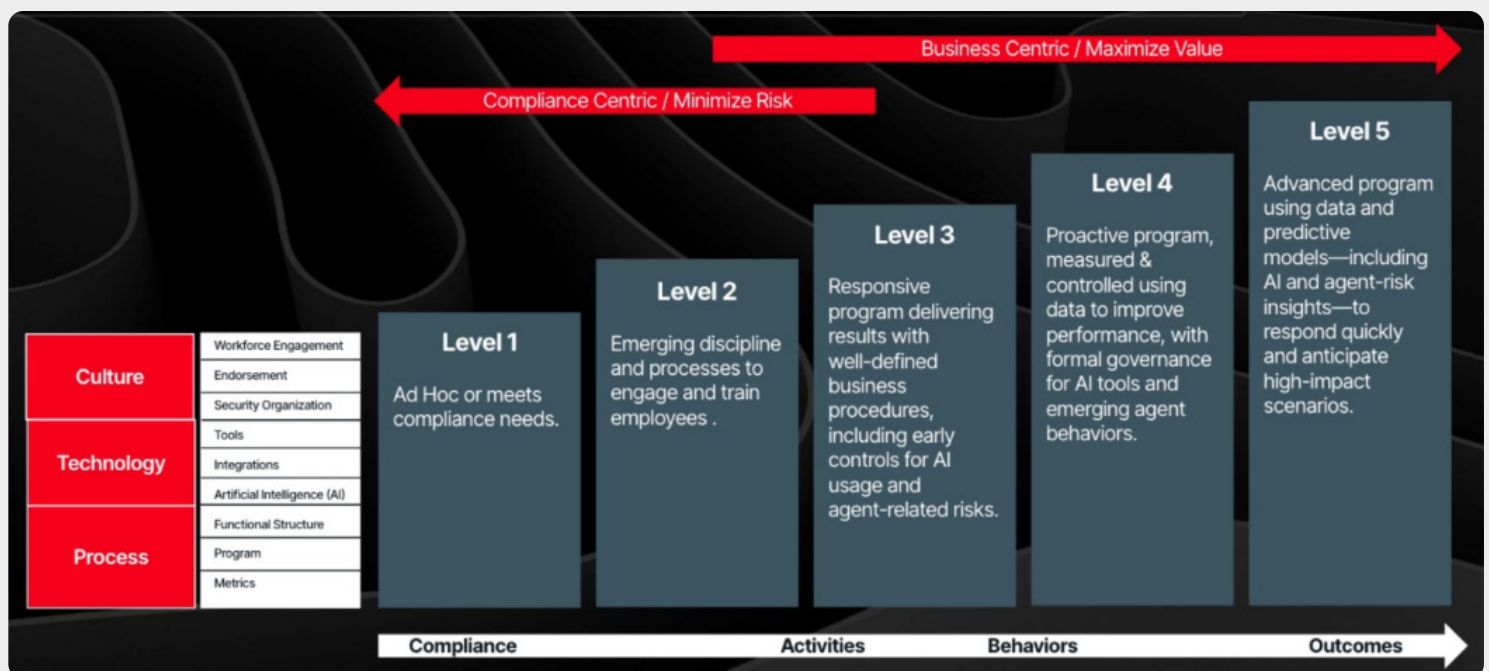
The Human Risk Management Maturity Model provides a structured path forward — from reactive compliance to predictive, AI-powered governance.

Explore the full Human Risk Management Maturity Model framework, including detailed benchmarks across Culture, Technology, and Process:

<https://www.livingsecurity.com/hrm-maturity-model>

This framework positions HRM not as a disruptive replacement for Security Awareness Training, but as its natural evolution. As organizations progress through the stages, they move:

- From activity to outcomes
- From completion metrics to exposure measurement
- From isolated training programs to integrated risk governance
- From reactive remediation to predictive prevention



If you are unsure where your organization stands today, the following readiness diagnostic can help quantify your current maturity level and identify your next step forward.

HRM Readiness Diagnostic (Scored Assessment)

Instructions

Rate each statement from 0–3:

0 = Not in place **1** = Limited / ad hoc **2** = Partially implemented **3** = Fully operational

Risk Visibility & Measurement

#	Statement	Score (0–3)
1	We can quantify human cyber risk at the individual level.	
2	We can identify our highest-risk users at any given time.	
3	We track exposure duration (how long users remain in elevated risk states).	
4	We measure risk movement trends over time.	
5	Human risk signals are integrated with identity and endpoint telemetry.	

Intervention & Automation

#	Statement	Score (0–3)
6	Behavioral interventions are automated based on risk signals.	
7	Training is personalized by demonstrated risk.	
8	Managers receive visibility into team-level risk.	
9	Positive behaviors (e.g., threat reporting) are reinforced and tracked.	

Executive Governance

#	Statement	Score (0–3)
10	We can provide board-ready reporting on human risk reduction.	
11	Human risk metrics are tied to broader enterprise risk frameworks.	
12	Human risk influences dynamic access or control decisions.	

Total Score: _____ / 36

Scoring Interpretation

0–12: Level 1 — Compliance

13–20: Level 2 — Visibility

21–28: Level 3 — Intelligence

29–36: Level 4 — Predictive

Scores in the top range indicate organizations approaching Optimized and Innovating maturity.

Organizations scoring **below 21** are typically operating without measurable human risk governance and are strong candidates for HRM evolution.

Get Your Human Risk Score

Take your next step with Living Security's HRM Maturity Model — an interactive framework that helps you:

- Validate your current maturity stage
- Benchmark against industry expectations
- Identify targeted next steps toward intelligence and predictive governance

Explore the HRM Maturity Model <https://www.livingsecurity.com/hrm-maturity-model>

PROOF POINT:

"Living Security's HRM Maturity Model demonstrates that organizations evolve from tracking training completion to measuring outcome-based, risk-driven indicators—because effective governance requires measurable risk movement, not just participation."

Source: Living Security Human Risk Management Maturity Model Ebook <https://www.livingsecurity.com/hrm-maturity-model>

The Shift to AI-Native Human Risk Management

The move from Security Awareness Training to Human Risk Management was necessary. The move from traditional HRM to AI-native HRM is structural.

Legacy SAT platforms were built to deliver content and run phishing simulations. Reporting and basic risk scoring were layered on later. But adding analytics to a training system does not make it a behavioral intelligence platform.

Today, **you’re facing** threats that are adaptive, automated, and AI-assisted. Phishing is dynamically generated. Impersonation leverages synthetic media. Employees rely on AI copilots and autonomous workflows daily. Human behavior now intersects continuously with AI systems.

Periodic simulations and static scoring models cannot keep pace.

With an AI-native HRM platform, **you get** continuous ingestion of identity, endpoint, email, data, and collaboration telemetry, plus dynamic scoring and automated interventions in real time. It analyzes patterns across hundreds of behavioral signals, dynamically recalibrates risk scores, and triggers automated, context-aware interventions in real time.

It does not just report on risk. It learns from it.

Legacy Architecture vs. AI-Native Architecture

The difference is architectural, not incremental.

Aspect	Legacy SAT + Analytics Layer	AI-Native HRM Platform Architecture
Core System	Content Delivery System	Unified Behavioral Intelligence Engine
Phishing Simulation	Separate Phishing Simulation Engine	Integrated Behavioral Modeling Across Humans & Agents
Data Ingestion	Periodic Data Exports	Continuous Ingestion of Identity, Endpoint, Email, Data, Collaboration, AI Telemetry
Risk Scoring	Static Scoring Models	Dynamic Risk Recalibration Based on Contextual Signals
Intervention	Manual Reporting and Remediation	Automated, Policy-Aware, Real-Time Interventions
Integration	Limited, Siloed Integrations	Bi-Directional Integration with IAM, Endpoint, DLP, GRC, AI Governance
Exposure Duration	No Visibility into Time-at-Risk	Embedded Continuous Measurement & Reduction of Elevated Risk States
Intelligence	Intelligence Bolted On After the Fact	Intelligence is Native, Learning and Adapting Continuously

The platform does not simply report on risk. It learns from patterns, adapts scoring models, and continuously reduces exposure. This architectural distinction is what separates a content platform with analytics from a behavioral risk intelligence system.

The Expanding AI and Agentic Risk Surface

As organizations adopt AI copilots and agentic workflows, new risk surfaces emerge:

- Data exposure through AI prompts
- Shadow AI usage outside approved environments
- Blurred human and non-human identity boundaries
- Automation executing actions outside policy guardrails
- AI systems persisting context beyond individual sessions
- Autonomous workflows acting faster than human review cycles

These risks cannot be mitigated with annual training or phishing click rates. They require continuous behavioral modeling across both humans and the systems acting on their behalf.

AI-native HRM enables organizations to:

- Model human and AI-assisted behavior together
- Detect emerging risk patterns before incidents occur
- Reduce exposure duration automatically
- Deliver predictive, forward-looking risk reporting

This is not enhanced awareness. It is behavioral risk intelligence infrastructure.

The 12–18 Month Outlook: Why Waiting Is Risky

Over the next 12–18 months, three shifts are likely:

Timeframe	Milestone Description	
0–6 Months		AI-generated phishing becomes indistinguishable from legitimate communication.
6–12 Months		Static phishing simulations lose predictive value; attackers use advanced behavioral mimicry.
12–18 Months		Agentic automation gains delegated access to sensitive systems; non-human identities require risk scoring.
12–18 Months		Regulatory scrutiny expands to AI governance and workforce risk measurement.
12–18 Months		Boards demand continuous monitoring and reduction of human and AI exposure duration.

If you wait for a major AI-related incident before evolving your HRM architecture, you'll be forced into reactive, high-cost remediation.

If you adopt AI-native HRM now, **you build**:

- Continuous visibility into blended human-agent risk
- Adaptive controls that evolve with threat patterns
- Measurable reduction in time-at-risk
- Predictive insight that informs executive decision-making

As threats become more autonomous, human risk management must become more intelligent.

Human Risk Management must be AI-native to remain effective.

PROOF POINT:

"Forrester positioned Living Security as a Leader, highlighting its measurement of 250+ behaviors/events through 60+ out-of-the-box integrations and automated workflows that respond dynamically to risk."

Source: Forrester Wave™ Human Risk Management, Q3 2024
Read the Forrester Wave Report <https://www.livingsecurity.com/forrester-wave-report-2024>

PURCHASING MODELS:

All-in-One vs. Modular

You can adopt HRM in different ways depending on contractual flexibility, architectural strategy, and internal readiness. The decision is not simply about features. It is about whether HRM becomes your primary behavioral intelligence layer, or augments your existing stack.

Model 1. All-in-One HRM Platform

A comprehensive HRM platform includes:

- Training and phishing simulation
- Behavioral risk scoring
- Automated interventions
- Exposure duration measurement
- Executive reporting
- AI and agentic risk governance

Best suited for organizations:

- Replacing legacy SAT platforms
- Seeking vendor consolidation
- Standardizing user and administrator experience
- Embedding HRM into long-term security strategy

This model ensures tight integration across behavioral telemetry, scoring logic, and intervention workflows.

PROOF POINT:

"Forrester defines HRM as a distinct market beyond awareness training and phishing simulations, emphasizing telemetry-driven behavior measurement and risk-led interventions."

Source: Living Security Human Risk Management Maturity Model Ebook, <https://www.livingsecurity.com/hrm-maturity-model>

Model 2. Modular/Component-Based Deployment

Organizations may adopt HRM capabilities selectively while retaining portions of their existing stack.

Examples:

- Retain current SAT vendor, add HRM risk scoring and automation
- Maintain phishing simulations, integrate HRM behavioral analytics
- Pilot exposure duration tracking before broader consolidation

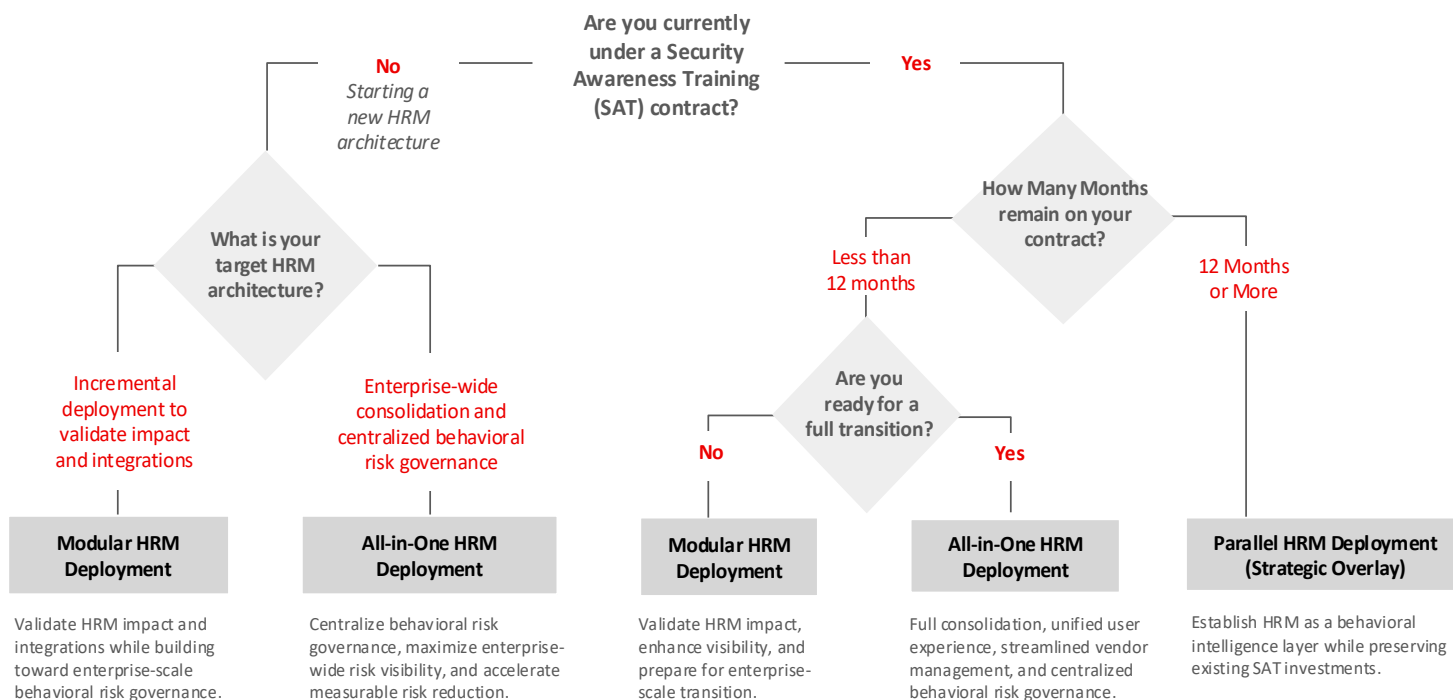
Best suited for organizations:

- Under active SAT contracts
- Seeking to pilot HRM before full migration
- Looking to enhance visibility without immediate rip-and-replace
- Testing business case validation before broader investment

HRM can function as a behavioral intelligence layer above existing training systems, adding measurable visibility and automation without disrupting current infrastructure.

Decision Tree: Choosing Your HRM Purchasing Model

The purchasing model should support your long-term risk architecture, not constrain it.



NEXT STEPS:

Moving from Awareness to Measurable Risk Reduction

If you expect to evaluate Human Risk Management in the next 12–18 months, the most strategic move is not waiting, it's gaining visibility now. As employees adopt AI copilots and autonomous workflows, and as attackers increasingly leverage AI-driven tactics, human risk becomes more dynamic, distributed, and adaptive. Static awareness programs were built for a different threat environment. AI-native Human Risk Management is built for this one.

Start by:

1. Conducting a Human Risk Readiness Assessment
2. Mapping current identity, behavioral, and AI-related telemetry sources
3. Identifying your highest-risk users and exposure duration trends
4. Determining whether modular or consolidated deployment aligns with your roadmap

Proven Impact

Organizations implementing AI-native HRM have demonstrated:

- Measurable reduction in high-risk user concentration within the first 60–90 days
- Executive visibility into exposure duration trends for the first time
- Automated intervention cycles replacing manual, spreadsheet-driven processes
- Board-ready reporting aligned to enterprise risk governance expectations

In one large healthcare organization, targeted automation and exposure duration tracking reduced elevated-risk user populations significantly within a single quarter, while operating alongside existing SAT contracts.

The result was not just improved training metrics. It was measurable risk reduction.

PROOF POINT:

"A Fortune 500 healthcare organization reduced high-risk user exposure duration by 58% within 90 days using Living Security's AI-native HRM platform, while operating alongside existing SAT contracts."

Source: Living Security Client Outcomes (anonymized)

Analyst Recognition

In *The Forrester Wave™: Human Risk Management Solutions, Q3 2024*, Forrester placed Living Security in the **Leaders** category and cited its progress in driving HRM adoption.

Forrester also notes Living Security's breadth in behavior detection (**250+ behaviors/events**) and integration coverage (**60+ out-of-the-box integrations**), plus automated workflows that respond to risky events.

Take the Next Step

Human risk is measurable. Human risk is manageable. And in an AI-accelerated threat landscape, it is continuously evolving. The question is not whether to evolve beyond awareness. The question is how quickly you can operationalize AI-native human risk intelligence.

To get started:

- Request a complimentary Human Risk Assessment
- Schedule a 30-minute Risk Visibility Demo
- Download the interactive HRM Readiness Scorecard

Visit: <https://www.livingsecurity.com/hrm-maturity-model>

Or contact our team to begin evaluating your current human risk posture.

