Jericho Security

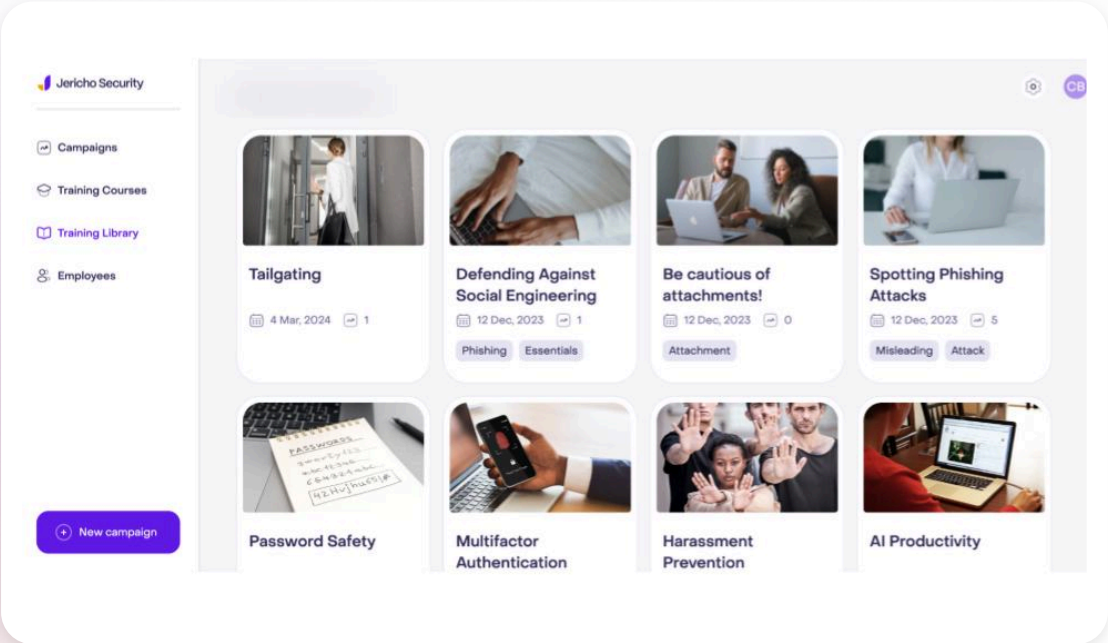
Modernizing Security Awareness for the AI Era

A KnowBe4 Alternative Buyer's Guide

The cybersecurity landscape has changed more in the past two years than in the previous decade. The rise of **generative AI** has transformed both the scale and sophistication of social engineering. Threat actors are using AI to create personalized phishing emails, deepfake videos, and cloned voices that can convincingly mimic executives and trusted brands.

Legacy awareness programs built on **static content libraries and manual campaign management** are ill-equipped for this new threat environment. Security leaders need awareness programs that evolve at machine speed, detect behavioral risks in real time, and adapt training dynamically based on user performance.

This white paper helps CISOs and security program owners evaluate alternatives to legacy awareness platforms such as KnowBe4. It outlines how **Jericho Security's AI-native approach** delivers dynamic, automated, and intelligence-driven awareness training designed for the realities of 2025 and beyond.



2. The Evolving Threat Landscape

AI as a Force Multiplier for Attackers

Generative AI models can create **hyper-realistic phishing campaigns** that bypass traditional detection and awareness filters. Attackers now deploy:

- AI-written spear phishing messages personalized by role or industry
- Deepfake audio for CEO fraud and wire transfer scams
- Synthetic identities for credential harvesting and insider impersonation

The cost of creating convincing phishing content has dropped to near zero. The barrier to entry is gone; threat actors can now scale social engineering faster than enterprises can train employees.

The Expanding Human Attack Surface

Employees remain the first, and often last, line of defense. But traditional annual or quarterly awareness training doesn't reflect how humans actually learn or respond to dynamic threats. Human risk must now be managed continuously, not periodically.

3. The Legacy Awareness Problem

Platforms like KnowBe4 pioneered large-scale phishing simulation and compliance-driven training. But they were designed for a different era; one defined by static content, predictable attacks, and human-curated campaigns.

Common Limitations of Legacy Programs

Static Phishing Templates

Simulations are reused, recognizable, and outdated within months.

One-Size-Fits-All Training

All users receive the same videos or quizzes regardless of role or risk.

Manual Campaign Management

Security teams spend hours scheduling, tracking, and reporting training events.

Shallow Metrics

Success is measured by completion rates or click percentages, not actual behavioral change.

Low Engagement

Users tune out repetitive, irrelevant content, leading to “training fatigue.”

The Result

Traditional awareness platforms have become compliance tools, not resilience engines. They fulfill audit requirements but fail to reduce real-world risk.

4. What Modern Security Awareness Means in 2026

The next generation of awareness programs must be intelligent, dynamic, and autonomous. CISOs are shifting their evaluation criteria from content quantity to learning quality and behavioral outcomes.

Key Principles of Modern Awareness

AI-Driven Threat Simulation

Simulations built from live threat intelligence mirror current attacker methods.

Hyper-personalized Learning Paths

Training adjusts automatically based on individual performance, role, and risk level.

Behavioral Analytics

Continuous measurement of user behavior identifies emerging risk trends.

Real-Time Reinforcement

Microlearning, nudges, and contextual reminders reinforce secure behavior daily.

Outcomes That Matter

- Measurable reduction in phishing susceptibility
- Increased employee vigilance and reporting behavior
- Reduced overhead for security teams
- Quantifiable alignment between awareness and enterprise security outcomes

5. Buyer's Framework: Evaluating Awareness Solutions in the AI Era

Evaluation Dimension	What to Look For	Why It Matters
AI Readiness	Real-time threat simulation, automated content generation	Keeps training aligned with evolving attack vectors
Automation & Adaptability	Campaigns that self-optimize based on performance data	Reduces manual workload and improves scalability
Behavioral Intelligence	Analytics that correlate user actions with risk signals	Moves beyond compliance to measurable resilience
Engagement & Culture	Campaigns that self-optimize based on performance data	Reduces manual workload and improves scalability
Data Privacy & Compliance	Campaigns that self-optimize based on performance data	Reduces manual workload and improves scalability

Jericho Security

6. KnowBe4 vs. Jericho Security: The Modern Alternative

	KnowBe4 (Legacy Model)	Jericho Security (AI-Native Platform)
AI Readiness	✕ Relies on static templates and human-curated content	✓ Uses generative AI to create threat-aligned simulations in real time
Automation	✕ Manual campaign setup and scheduling	✓ Fully automated phishing simulation and training delivery
Adaptiveness	✕ One-size-fits-all training	✓ Dynamic learning paths based on user behavior and risk
Threat Intelligence	✕ Limited integration	✓ Ingests live threat intelligence to mirror current attack trends
Behavioral Analytics	✕ Basic click-through reporting	✓ Deep behavioral telemetry and human risk scoring

Jericho Security

	KnowBe4 (Legacy Model)	Jericho Security (AI-Native Platform)
User Engagement	✕ Repetitive content leads to fatigue	✓ Personalized, contextual microlearning drives 3× engagement
Operational Overhead	✕ High administrative burden	✓ Automation reduces management time by 70%+
Business Outcomes	✕ Compliance-focused metrics	✓ Demonstrated 45% faster risk reduction and higher employee participation

The Jericho Advantage

Jericho Security's adaptive learning engine is built to evolve at the speed of AI. Instead of chasing the next phishing template, Jericho continuously generates context-aware simulations based on global threat intelligence. The platform learns from user interactions, adjusting difficulty, delivery timing, and reinforcement automatically.

7. Conclusion and Buyer's Checklist

Key Takeaways

1. The threat landscape now evolves faster than traditional awareness platforms can update.
2. AI-driven attackers require AI-enabled defenders.
3. Modern security awareness must be personalized, data-driven, and continuous.
4. Jericho Security represents a new category of AI security awareness; turning every employee into an intelligent sensor and resilient participant in security operations.

Buyer's Checklist for the AI Era

When evaluating your next security awareness partner, ensure the solution can:

- Automatically simulate AI-generated phishing attacks
- Deliver hyper-personalized training tailored to role and risk level
- Integrate with your existing SIEM and identity stack
- Provide real-time behavioral analytics and human risk scoring
- Offer continuous microlearning reinforcement
- Reduce operational overhead through automation
- Demonstrate measurable improvements in resilience metrics

8. About Jericho Security

Jericho Security is the leader in **defense-grade AI security awareness and human risk management**. Built for the modern enterprise, Jericho uses generative AI and live threat intelligence to deliver dynamic, hyper-personalized training, real-time phishing simulations, and continuous behavioral insights. By replacing static content with dynamic learning experiences, Jericho enables organizations to build a culture of security resilience, at the speed of AI.

For more information visit
www.jerichosecurity.com