EBOOK

The five must-haves of modern human risk management

Cybersecurity has evolved, but many of its tools haven't. We're in an arms race of sorts, with attackers using AI to get faster, smarter, and more targeted.

Fable

Table of contents

Mitigating human risk: A strategic imperative

Cybersecurity has evolved, but many of its tools haven't. We're in an arms race of sorts, with attackers using AI to get faster, smarter, and more targeted.

Security professionals try to fend them off with AI of their own, but organizational defenses have focused largely on infrastructure and endpoints, not people. Attackers are exploiting this, and largely succeeding. Indeed, human behavior remains the single largest driver of security incidents, accounting for more than two-thirds of successful attacks, according to most studies.

Human risk lies in everyday behavior: a rushed click, a reused password, a forgotten update on a personal device. Today's human risk management solutions fall short. They rely on generic training and clunky awareness campaigns. The open secret among security teams and corporate employees alike is—despite receiving training and phishing simulations on a regular basis—these broad-based approaches don't work. According to a recent study on security awareness training, half of training sessions end within 10 seconds and fewer than 24 percent of users formally complete the training materials.

As organizations invest in next-generation cybersecurity, they can't afford to ignore the human layer. Mitigating human risk is no longer a nice-to-have; it's a strategic imperative that impacts the bottom line of every business. In this paper, we outline five essential capabilities of human risk management programs—ones that shape behavior directly and drive real outcomes. We also overlay them on a simple maturity model to give you a sense for your human risk management roadmap and progress.

Data-driven

Synthesizes risk from employee behavior data from first and third parties, and takes action based on that data.

Highly-targeted

Generates customized, risk-based simulations, training, and behavioral interventions.

Just-in-time

Delivers interventions in the moment of risky behavior or emerging threat, right where people work.

Outcomes-focused

Produces measurable, continually-improving outcomes, such as reduced susceptibility to social engineering or improved handling of sensitive data.

Enterprise-grade

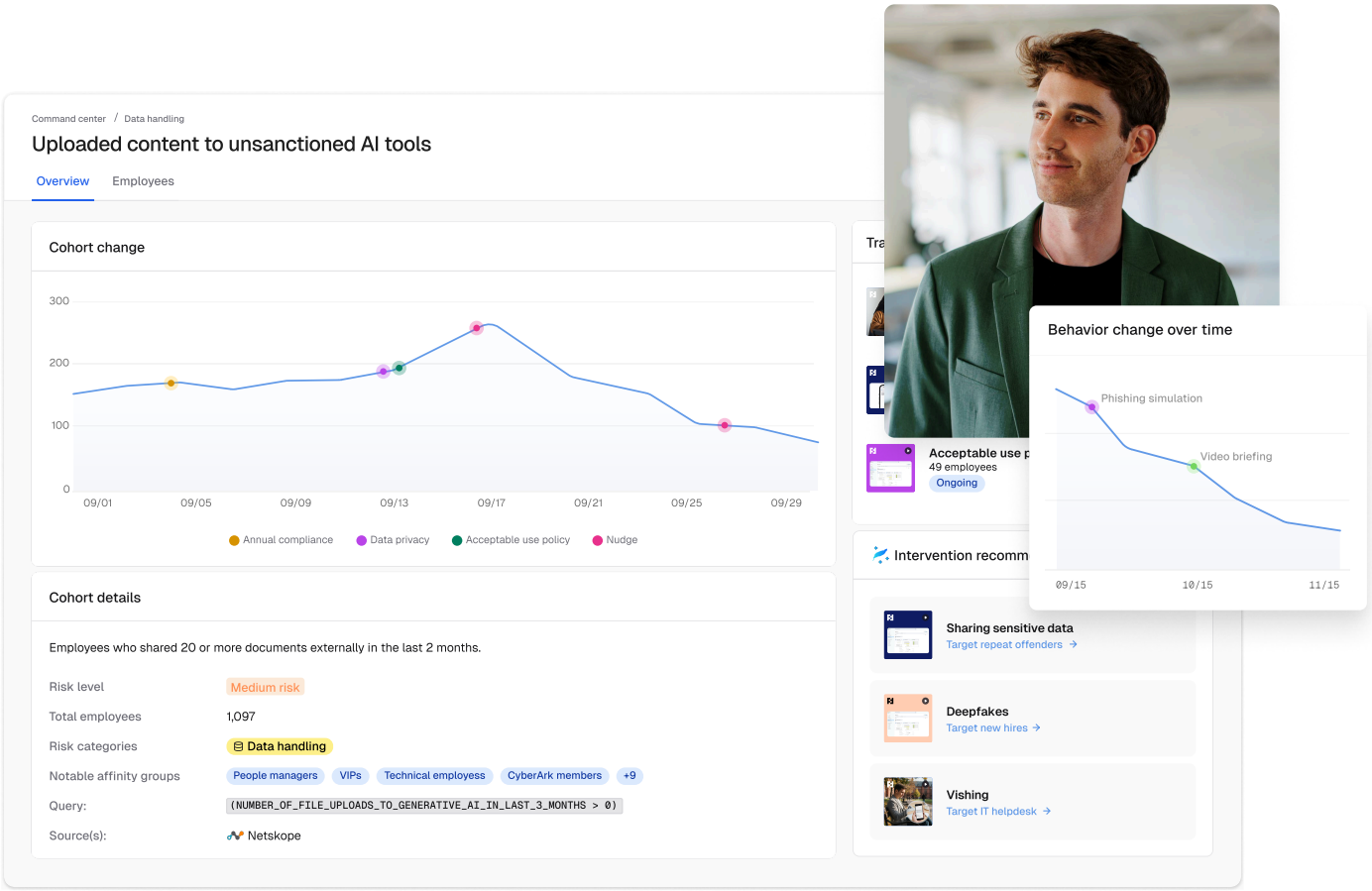
Snaps seamlessly into the enterprise stack and is scalable, secure, automated, and simple to administer.

[1] Ho, Mirian, Luo, Tong, Lee, Liu, Longhurst, Dameff, Savage, Voelker. "Understanding the Efficacy of Phishing Training in Practice." UC San Diego, University of Chicago, UC San Diego Health, 2024.

MUST-HAVE #1

Data-driven

Existing human risk management solutions are often untethered from the human behavior gaps that need to be addressed.



Organizations miss out on the opportunity to deliver, say, a briefing on a breaking vishing scam to money handlers in a financial firm. This gap is especially disappointing given enterprises are awash in all manner of data—breach notifications, vulnerability announcements, network telemetry, access logs, behavior metrics, and more—and it's easier than ever to integrate and analyze data with data lakes and visualization tools.

It should synthesize risk based on both first- and third-party signals—and taking action on—human risk. The program should be based on first-party signals from training programs and phishing simulations, as well as third-party ones from enterprise workspaces, human resource systems, identity and access management solutions, communications platforms, cloud and endpoint security products, and more.

It's not just a question of collecting this data, but building the model that accurately parses, weights, and synthesizes these data points into an ongoing risk score. From there, professionals should be able to narrow down risk scores by groups of people, as well as drill in to see risk factors and details.

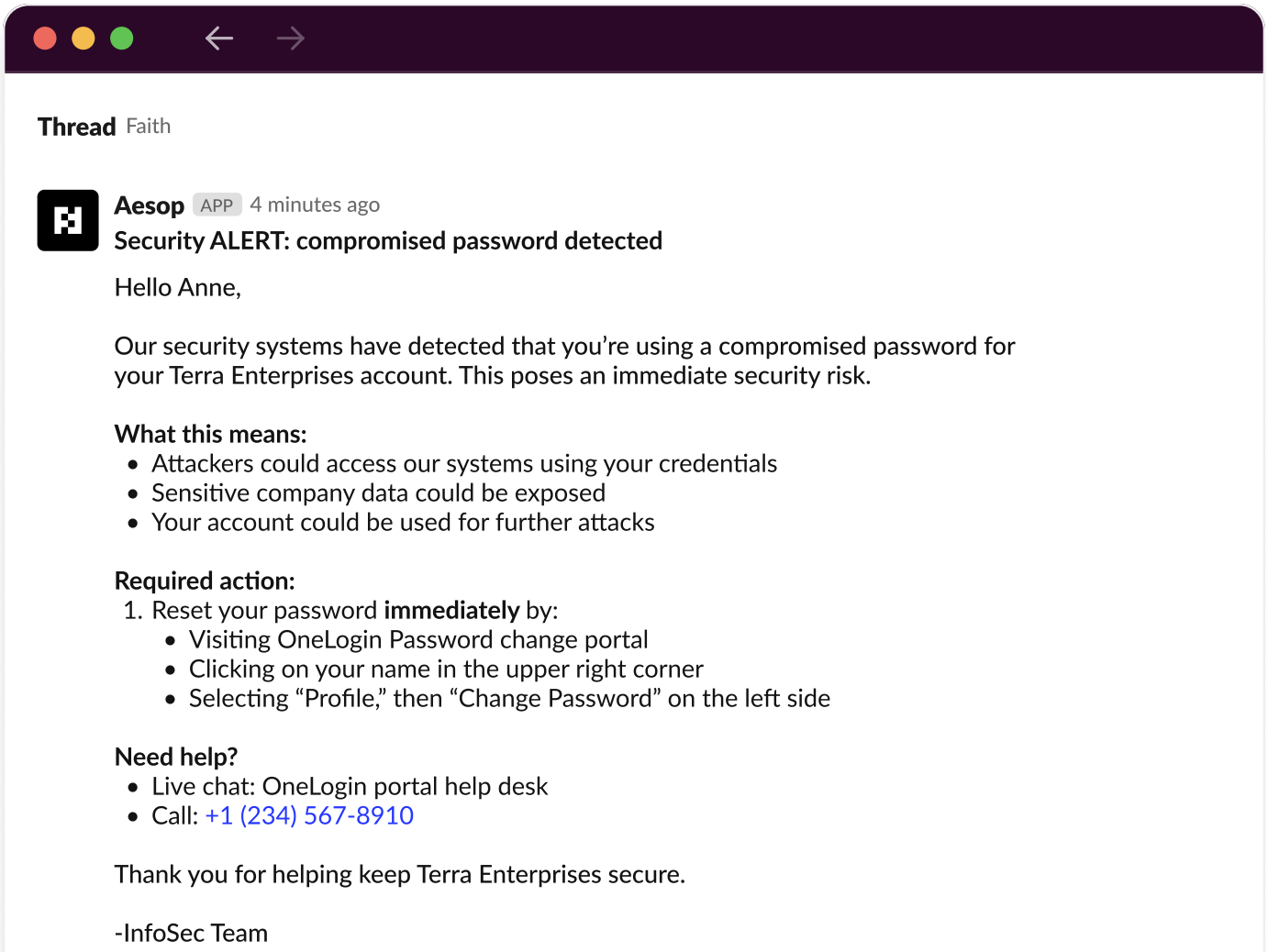
> With our human behavior index, we synthesize thousands of real-time employee behavior signals from systems across the enterprise.

With our human behavior index, we synthesize thousands of employee behavior signals from systems across the enterprise—identity and access, human resource, workspace, and security systems—identifying where gaps in human behavior introduce risk into the business.

From there, our risk engine layers in business and employee context to generate a comprehensive risk score, and breaks it down among factors that comprise that score. Security professionals can drill in to understand risk at the individual, cohort, business unit, or organization level, as well as deploy AI interventions—such as personalized video briefings—in a data-driven way.

Highly-targeted

Most human risk management solutions rely on generic training and periodic, one-size-fits-all social engineering simulations. While these may satisfy compliance requirements, they often fall short of meaningfully reducing risk.



Thread Faith

Aesop APP 4 minutes ago

Security ALERT: compromised password detected

Hello Anne,

Our security systems have detected that you're using a compromised password for your Terra Enterprises account. This poses an immediate security risk.

What this means:

- Attackers could access our systems using your credentials
- Sensitive company data could be exposed
- Your account could be used for further attacks

Required action:

1. Reset your password **immediately** by:
   - Visiting OneLogin Password change portal
   - Clicking on your name in the upper right corner
   - Selecting "Profile," then "Change Password" on the left side

Need help?

- Live chat: OneLogin portal help desk
- Call: +1 (234) 567-8910

Thank you for helping keep Terra Enterprises secure.

-InfoSec Team

Take, for example, an employee on the finance team whose operating system is missing a critical security patch: broad training on phishing or device hygiene does little to address that exact vulnerability. Or take an HR employee who uses Workday, but receives a phishing simulation from a different HR tool than what they use (or a generic one). That's a missed opportunity to target employees with just the right content. Even platforms with large libraries of specialized modules face usability challenges: content can be hard to find, outdated, or irrelevant by the time it's used. Changes can require months, so they're too-little, too-late for policy changes or to address emerging threats. Beyond being scattershot, most content also fails to stick. That's because it's rarely personalized, seldom aligned to people's roles, and almost never mapped to a specific behavior. This makes it easy to ignore and hard to apply when it counts.

Changes can require months, so they're too-little, too-late for policy changes or to address emerging threats. Beyond being scattershot, most content also fails to stick.

What's needed is a highly-targeted approach to addressing risk. Programs should deliver precise, relevant simulations, training, and behavioral interventions—both in form and content. AI makes this possible by identifying issues, determining the right response, and scaling that response through mass customization. Security teams should be able to use this capability to take corrective action, such as urging the finance employee to install the security update the moment it's available, or pushing a hyper-relevant Workday phish to the HR employee.

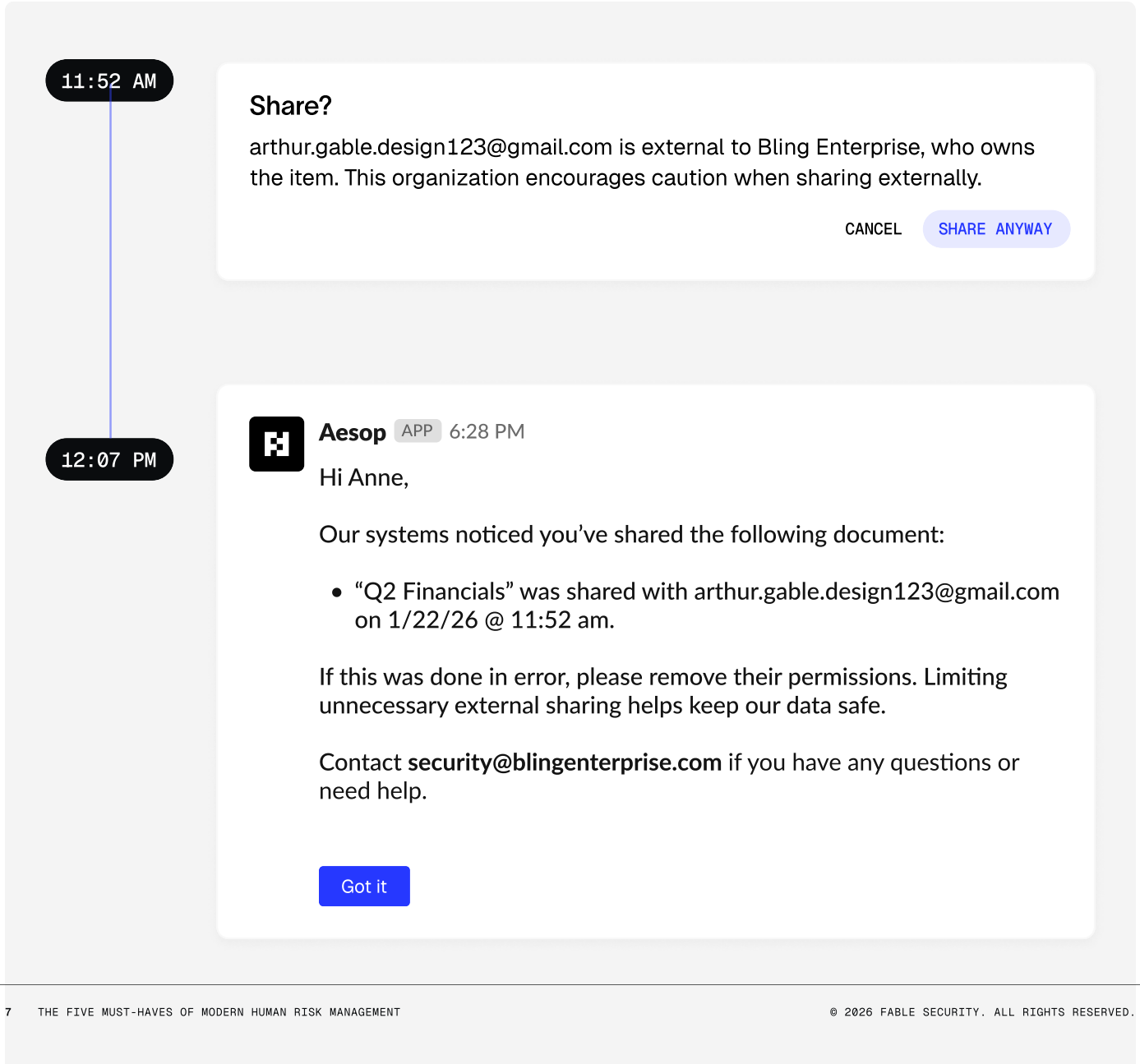
...automatically deploy interventions, delivered one-to-one to employees.

Fable features highly-targeted agentic interventions that address specific risks. Security professionals can automatically deploy AI-generated video briefings, small nudges, or two-way chats, delivered one-to-one to employees. Each intervention is customized with details about the employee's role, system access, and behavior, as well as customized with organizational policies, context, and concrete calls to action. Most importantly, Fable makes it simple to do this in just a few clicks through a clear, streamlined user interface.

MUST-HAVE #3

Just-in-time

Fable delivers targeted, just-in-time interventions to people based on their risky behavior, right to their email, text, messenger, or in-app.



Traditional human risk management solutions lean heavily on generic, scheduled training—typically once or twice a year, supplemented by occasional reminders or phishing simulations. These programs not only lack relevance to specific risks, but also fail to reach people in a timely manner. For example, a developer who accidentally embeds API keys in code can cause serious damage if they aren't alerted immediately. Research conducted in the early 1900s, and reinforced in subsequent experiments, shows that lessons are unlikely to stick even a few days after they're delivered. So, unless interventions happen quickly, people may not remember the good security behaviors they learned, leaving systems and data exposed.

Unless interventions happen quickly, people may not remember the good security behaviors they learned, leaving systems and data exposed.

What's needed is a program that not only addresses specific risks, but does so quickly, in response to risky behaviors—and right where people work.

Fable delivers targeted, just-in-time interventions to people based on their risky behavior, right to their email, Slack, or Teams. By targeting specific risks as soon as they're detected, we're able to get people's attention and prompt meaningful behavior change right when it matters most—and deliver a sticky message that lasts. Beyond delivering interventions quickly, we make it easy for administrators to automate follow-up timing, frequency, and channel.

[2] "Memory; a contribution to experimental psychology." Ebbinghaus, Hermann, 1913.

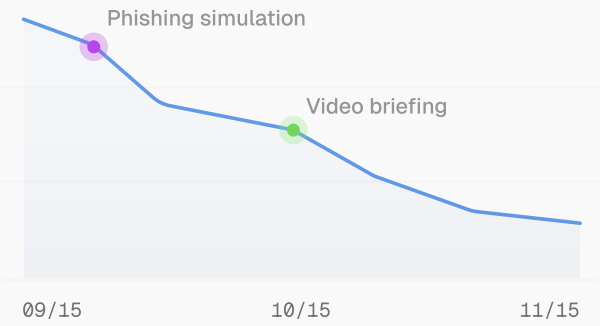
Outcomes-focused

Our customers describe measurable improvements in security behavior, from decreasing phishing clicks by 86% to reducing PII exposure by 60%, to shrinking time-to-behavior change from weeks to hours.

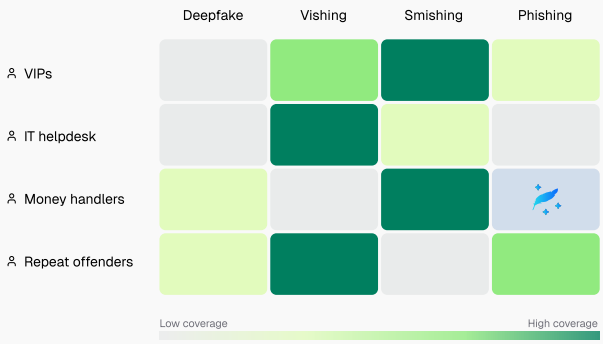
Simulations deployed
12

Reporting rate
65% ↑ since last month

Behavior change over time



Threat coverage



EvilAI briefing
3 days ago

★★★★★

Will keep an eye out for this!
Nice video—short and to-the-point.

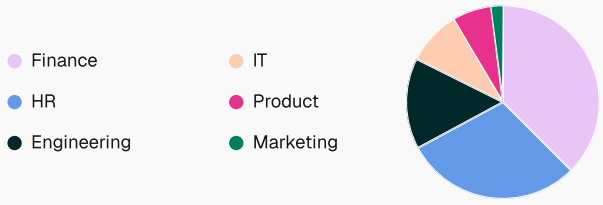
Relevant to me | Thumbs up

Employees with largest risk variance

AC	Avery Chen	Risk Analyst
JS	Jamie Silva	Security Engineer
DK	Dakota Kim	Head of Compliance

Employees sharing sensitive data

Risk across affinity groups



Human risk management has long struggled to show meaningful security outcomes or a clear return on investment. Security training is seen as a nuisance—generic, disconnected from real-world events, and too superficial to affect how risks actually play out in corporate environments. Indeed, security teams cite compliance as the real driver for investing in awareness training and phishing simulations. These efforts are rarely justified on security ROI alone—and some research even suggests they may do more harm than good.

What's needed is an approach that focuses on changing behavior. It should deliver interventions that actually work—because they target the right behavior, in the right place, at the right time. Beyond changing behavior, the program should also measure that change (e.g., percent reduction in social engineering clicks, exposed data, or time to update an OS) and incorporate a feedback loop for continuous improvement.

With a laser focus on shaping behavior directly, Fable embodies outcomes-focused human risk management. Our customers describe measurable improvements in security behavior, from decreasing phishing clicks by 86% to reducing PII exposure by 60%, to shrinking time-to-behavior change from weeks to hours. Fable hasn't just achieved category-defining returns for its security customers, but has enjoyed accolades from employees themselves, including a cumulative rating of 4.8 stars.

86%
decrease in phishing clicks

60%
reduction in PII exposure

4.8/5
Fable's cumulative rating by customers' employees

[1] Ho, Mirian, Luo, Tong, Lee, Liu, Longhurst, Dameff, Savage, Voelker. "Understanding the Efficacy of Phishing Training in Practice." UC San Diego, University of Chicago, UC San Diego Health, 2024.

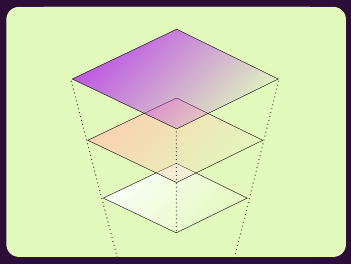
MUST-HAVE #5

Enterprise-grade

Many human risk management tools function as siloed solutions: standalone modules in an organization's LMS, disconnected from the broader enterprise stack.

Integrated into your tech stack

Get 50+ out-of-the-box integrations and a robust API so you can snap Fable easily into your identity framework, business applications, security tools, and support systems.

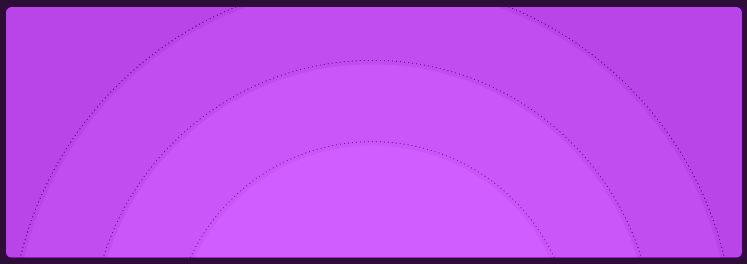


Scalable

Manage human risk across large, complex environments. Our scalable architecture, data lake, analytics engine, and support for custom branding and localization make it easy.

Secure by design

Be confident in our secure architecture and rigorous data-handling. We enforce strict security policies, least-privilege access, and thorough audits to protect your data.



Simple to administer

Don't sweat the administrative burden. We make it easy for you to configure global settings, assign fine-grained access, automate campaigns, and be audit ready.

They fall short when it comes to the day-to-day realities of large organizations: complex structures, varied user roles, regulatory obligations, global operations, and the need for clear oversight. Imagine a large enterprise trying to deploy a security awareness initiative across regions, only to find that the platform doesn't support localization, lacks role-based access, or requires cumbersome manual administration. Anybody who has administered one of these old-school solutions knows how impossible they are to manage at the scale of a modern, distributed enterprise. They require so much manual intervention to set up, run, and maintain that they usually fall behind the enterprise's needs—and end up delivering outdated training selected years ago because the team simply couldn't keep up, even as threats have evolved apace. In an environment where simplicity, scale, and security are non-negotiable, these limitations become blockers —not just for security progress, but for adoption itself.

What's needed is a solution that meets enterprise-grade expectations out of the box.

What's needed is a solution that meets enterprise-grade expectations out of the box. That means seamless integration into the existing ecosystem, with robust APIs and SSO support. It means administrative simplicity paired with sophisticated controls: role-based permissions, audit logging, and global configuration management. It also means operational readiness —localization for global teams, brand customization for internal alignment, and the kind of reporting, compliance posture, and support experience that security leaders expect from any core enterprise platform.

Fable was built for the enterprise from day one. Our platform is simple to administer, globally scalable, and secure by design. Security teams can configure global settings, assign permissions with fine-grained, role-based access, and maintain audit readiness with robust logging and reporting. We support automated campaign creation with AI-generated recommendations and interventions, custom branding, localization, and seamless integration with your existing stack —along with white-glove implementation and world-class support to ensure success across the organization.

Maturity across the five must-haves

How do you know where to begin with these five must-haves of modern human risk management? Use this simple framework to assess where your organization stands today and to chart your path forward.

	LOW	MEDIUM	HIGH
DATA-DRIVEN	Manual (or no) risk calculation, untethered from training	Periodic risk calculation that informs manual interventions	Dynamic, comprehensive risk scoring that drives automated interventions and measures behavior change
HIGHLY-TARGETED	Generic training and one-size-fits-all phishing simulations	Manual interventions based on role and risk	Targeted, personalized, customized AI interventions based on risk
JUST-IN-TIME	Periodic delivery	Delivery in response to role and risk	Delivery as soon as risky behavior is detected, right where people work
OUTCOMES-FOCUSED	Compliance checkboxes	Risk reduction	Behavior change, measurable ROI, and enthusiastic employee feedback
ENTERPRISE-GRADE	Standalone training modules	Some enterprise integration, enterprise features, and basic reporting	Robust enterprise integration, security built-in, automated campaign creation and deployment, and audit-ready reporting

In summary

Modern human risk management requires more than check-the-box training and simulations.

Modern human risk management requires more than check-the-box training and simulations. To keep up with increasingly sophisticated, AI-driven threats and drive real change across their employee bases, organizations need solutions that are data-driven, highly-targeted, just-in-time, outcomes-focused, and enterprise-grade.

By embracing these five must-haves, security teams can move beyond compliance toward actual risk reduction—addressing the right behaviors at the right moments with the right interventions to change behavior and drive security resilience across the organization. Fable was built to deliver on this vision, giving organizations the intelligence, precision, and enterprise scale needed to transform human risk management into a successful part of their security program.

FABLESECURITY.COM
HELLO@FABLESECURITY.COM

Fable