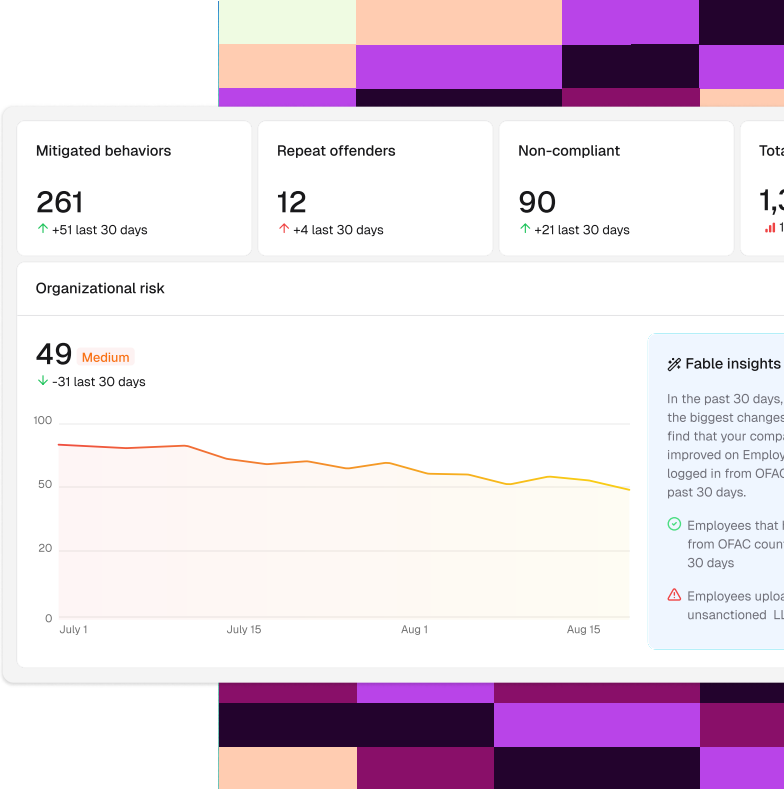
Human risk, meet your match

Despite spending billions on cybersecurity, organizations remain vulnerable to cyber attack. Fueled by AI, cyber threats are more numerous and sophisticated than ever.

We've reimagined human risk management with the best of AI. With Fable, you can deliver hyper-targeted phishing simulations, awareness training, and behavioral interventions—and report with confidence.



Phishing simulations

Realistic, AI-generated campaigns targeted by role, risk, and threats.

Awareness training

Infinite library of templates to personalize and customize with AI.

Behavioral interventions

Hyper-targeted AI interventions (videos, nudges, and chats).

Human risk reporting

Explainable risk reporting with dynamic scoring, drill-downs, and insights.

PENNYMAC

Pennymac used Fable to prompt a high-priority behavior change.

What normally takes five days took four hours and saved 105+ SOC hours.

4 hrs

time to behavior change

105+

SOC hours saved on a single campaign

"As Fable engagement went up, vulnerabilities went down. We could measure the effectiveness of the campaign."

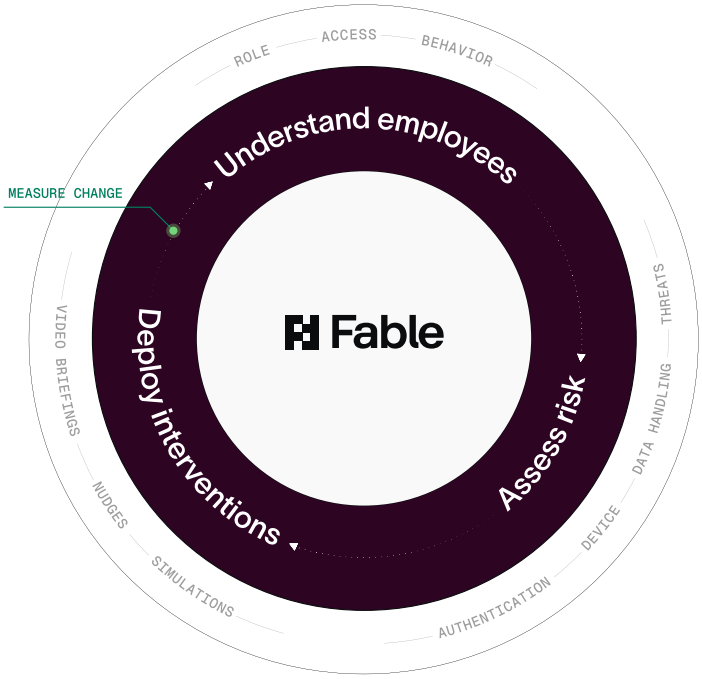
Cyrus Tibbs
CISO at Pennymac

Fable

HOW FABLE WORKS

We shape employee behavior in three simple steps

We understand employees, assess risk, and deploy AI interventions—driving measurable behavior change.



Understand employees

- Synthesize third-party and Fable data
- Resolve attributes to each employee
- Understand behavior and context

Assess risk

- Build employee risk profile
- Create risk cohorts
- Recommend interventions

Deploy interventions

- Auto-generate interventions with AI
- Create video briefings, nudges, and chats
- Deliver to Slack, Teams, GChat, and email

Simplicity and enterprise scale

Ease of administration

Don't sweat enterprise complexity. We made administration effortless, with automated content creation and campaign management.

Enterprise security

Be confident in our security posture. We enforce strict policies, least-privilege access, and secure data-handling processes.

Integration

Snap easily into your identity framework, business applications, security tools, and communications systems with out-of-the-box integrations.

Assess risk in a data-driven way

CAPABILITY	VALUE
Data ingestion	Synthesize employee signals from identity, HR, workspace, and security (application, device, cloud, email, and network).
Risk assessment	Synthesize risk with a dynamic, closed-loop process. Segment by employee, cohort, business unit, department, or organization.
Unified employee profile	See unified view of employee profile from disparate data sources for accurate risk analysis and reporting.
Smart group automation	Create employee groups (cohorts) automatically from attributes and behaviors for easy measurement and campaign delivery.
Board-ready reporting	Report on enterprise risk with filterable, explainable dashboards featuring departmental views, risk factors, and AI-driven insights.
Recommended interventions	View problematic behaviors and areas of disproportionate risk, and see prioritized intervention recommendations.
Employee sentiment	Capture employee rating and feedback post-interaction for continuous improvement. Current average = 4.8/5.

Conduct modern, adaptive phishing simulations and customized follow-up training

CAPABILITY	VALUE
Modern, relevant simulations	Target phishing simulations to employees' roles, behaviors, cohort attributes, and emerging threats.
Customized simulation	Customize your simulation—name, subject, content, images, fonts, buttons, flags, links, pages, variables, and HTML.
Phishing report integration	Integrate with phishing report mailboxes for agnostic reporting by all employees.
Infinite templates	Start with a robust template library, then use AI to automate endless variations for every difficulty or motivation.
Simulation types	Choose from a variety of test types—click, attachment, credential, double-barrel, and QR code.
Brand spoofing	Use brand- and situation-specific starter templates, or use AI to create your own easily.
Flexible scheduling	Choose campaign start date, time, and duration, and optimize for global time zones.
Simultaneous campaigns	Deliver a variety of highly-targeted campaigns to your employees simultaneously.
Post-fail education	Deliver immediate, tailored education after an employee fails a simulation to reinforce awareness and reduce repeat failures.
No bot clicks	Ensure delivery and clean data by allowlisting phishing simulations and filtering bot clicks from results.
Simulation reporting	Report on phishing simulation metrics, including percent open, failure, and data entry, time to report, and more.

Integrate human risk into your technology stack

CAPABILITY	VALUE
Workspace integrations	Integrate with identity, HR, workspace, and security (application, device, cloud, email, and network).
SCORM integration	Integrate with your SCORM-based learning management system for a seamless training experience.
Collaboration integrations	Integrate with Teams, Slack, GChat, and email to deliver just-in-time interventions right where people work.
Robust API	Use API for data ingestion and workflow automations.
Data export	Export human risk data and training/campaign results for external reporting and analytics.
Employee management	Upload employee CSV lists as an alternative or precursor to directory-based integration.

Rely on an enterprise-grade platform

CAPABILITY	VALUE
Data architecture	Ingest, normalize, and prime employee data in a centralized lakehouse for scalable analysis and machine learning.
Campaign automation	Administer trainings, simulations, and personalized interventions in a few clicks, no matter how complex your organization.
Policy mapping	Ingest and map policy documents to behaviors. Update risk models with compliance insights and contextual alignment.
Data security	Encrypt data using AES-256+ at rest and TLS 1.3+ in transit, ensuring robust protection standards.
Role-based access	Enable role-based access and control through integration with enterprise directories and single sign-on.
Data access	Gain read-only access to integrated data sources (e.g., directory, HR, and security products; metadata only; no access to email).
SSO support	Enable seamless, secure access through single sign-on integration, reducing friction and strengthening authentication across systems.
Audit logging	Log all user and administrator actions in a tamper-resistant way, exportable for compliance, investigations, and SIEM integration.

Train employees with targeted content

CAPABILITY	VALUE
Training content library	Choose from a library of customizable, brandable templates on a variety of topics, including for Cybersecurity Awareness Month.
SCORM exportability	Export all training modules for seamless compatibility with your learning management system.
Adaptive content	Adapt content based on employee risk, ensuring applicability and avoiding duplicate assignments.
Relevant training	Provide training modules to role and other attributes, such as access, business unit, tenure, location, and more.
Threat warnings	Train on recent attacks and threats with information about attackers, methods, and calls-to-action.
Personalized follow-up	Deliver automated, personalized training nudges that drive timely completion and sustained employee engagement.
Manager escalation	Reinforce accountability and ensure timely training completion with manager escalation workflows.
Multi-lingual support	Deliver region-specific content incorporating dialects, region-specific threats, and cultural norms.
Compliance-ready reporting	Report on training metrics, including assignments, progress, completions, and more.

Shape behavior with timely interventions

CAPABILITY	VALUE
Multi-modal content	Deliver content in a variety of modes—nudges, video briefings, and two-way chats—to fit any need.
Hyper-targeted interventions	Auto-generate hyper-targeted interventions—personalized with behavior, context, and next steps—only to those who need them.
Timely delivery	Deploy interventions when they're most impactful, as soon as risky behavior is detected.
Multi-channel reach	Choose from content delivery options, including Slack, Teams, GChat, email, or a mix.
Emerging threat defense	Defend against emerging threats, arming employees with real-time intelligence about attacks on similar organizations.
Dynamic follow-up	Ensure timely behavior change through automated follow-ups and manager escalations.
Intervention reporting	Report on intervention metrics, including delivery, consumption, behavior change, risk reduction, and employee feedback.