Understand intent, not just activity

Most security tools tell you what happened. Ent helps security teams understand why it is happening and intervene before it becomes an incident. As work moves across SaaS apps, browsers, AI tools, and agents, productivity itself has become the attack surface.

Ent combines endpoint-native telemetry with AI reasoning to understand behavior, role, and context in real time. When risk emerges, Ent applies the right level of friction: a warning, justification prompt, redaction, policy action, or SOC escalation. The result is fewer false positives, faster investigations, and protection that works where work happens.

The missing layer

Existing tools often see isolated signals, such as a process, a file, a login, a network event, or a policy violation. Each layer of the security stack covers a different slice of activity:

Security layer	What it sees
EDR	Process activity
IRM	Activity recording and case documentation
DLP	Governed data flow
UEBA	Aggregated patterns after the fact
SIEM	Alert correlation

Intent helps drive full-picture understanding. Ent sees the sequence around the action, which is what makes intent possible to understand, so organizations can distinguish legitimate work from risky behavior.

What Ent enables

Defensible AI adoption without blocking productivity: Help employees use AI tools and emerging workflows while keeping policy, data exposure, and risk in view.

In-the-moment guidance and intervention: Apply context-aware warnings, justification prompts, redaction, guided action, or blocking where supported.

Lower false positives with intent-aware context: Attach natural-language intent context to alerts so analysts can focus on meaningful risk instead of activity-only noise.

Behavioral context from day one: Understand user behavior, role, workflow, and endpoint activity without waiting weeks for baselines to mature.

Faster investigations with audit-grade evidence: Turn risky activity into visual timelines with annotated explanations that SOC, HR, Legal, and Compliance teams can understand.

Use cases

AI and app usage control

Get visibility into AI usage across supported browser, desktop, and workflow surfaces, including sensitive content typed, pasted, or uploaded into AI tools.

Last-mile threat prevention

Stop the click that starts the attack: ClickFix, fake browser updates, and social engineering disguised as normal work.

Insider risk management

Distinguish risky behaviors from user mistakes, intervene at the moment of risk, and preserve visual, annotated evidence for SOC, HR, and Legal.

AI and endpoint data loss prevention

Augment DLP for AI, browser, clipboard, and endpoint data movement traditional tools may miss.

Platform capabilities

Endpoint behavioral context

Captures security-relevant telemetry across supported apps, AI tools, browsers, clipboard, focus, files, workflows, and endpoint activity.

Intent-aware policy engine

Evaluates activity in context: who the user is, what they are doing, what is normal for their role, and how the action maps to organizational policy.

Right-friction interventions

Applies proportional response: warning, justification prompt, redaction, guided action, SOC escalation, or block where supported.

Visual investigations with evidence timelines

Presents the sequence of activity in plain language: user, action, application, workflow, destination, risk rationale, triggered policy, and recommended next step.

Stack enrichment

Enriches SIEM, EDR, and SOC workflows with endpoint behavioral context and intent-aware signal.

Deployment flexibility

Ent is designed to fit into existing security environments and supports flexible deployment models based on customer operational and data-boundary requirements. A single lightweight user-space agent is designed to coexist with EDR and SIEM.

Deployment options: SaaS (Ent-managed) · Customer-managed (self-hosted)

Supported cloud platforms: AWS · Microsoft Azure · Google Cloud Platform

Endpoints: Windows · macOS · Linux · major enterprise browsers

Company & founders

Ent was founded by Elias Manousos and Brandon Dixon, co-founders of RiskIQ (acquired by Microsoft) and members of the team behind Microsoft Security Copilot.

Ent is deployed with Global 2000 customers across hospitality, financial services, and defense, and is backed by Decibel, Sequoia, Crosspoint Capital, Craft Ventures, Shield Capital, Felicis, and In-Q-Tel. Schedule a demo to see how Ent fits into your existing security architecture.

Visit us at ent.ai