Protect work as it happens

Intent-aware AI endpoint security solutions overview

Security for human and agentic work

AI has changed how work happens. People now work alongside AI agents that act on their behalf, often faster than anyone can review each step. This helps organizations move faster. It also makes it harder to tell when everyday work starts to create risk.

> The Verizon 2026 Data Breach Investigations Report found that the human element was involved in 62% of breaches.

The same action can mean very different things depending on who takes it and why. An employee might paste confidential information into an unapproved AI tool. A departing worker might copy company data to a personal account. An attacker might trick someone into running a harmful command.

Most security tools can tell organizations what happened, usually after the fact. Ent helps them understand why it is happening and step in before a risky action becomes an incident.

Source: Verizon 2026 Data Breach Investigations Report Executive Summary

How Ent helps prevent risk without slowing work

Ent is the AI endpoint security platform for human and agentic work. Instead of looking at each action on its own, Ent looks at actions together to understand intent: what a person or AI agent is trying to accomplish, based on the actions surrounding their work.

That context makes a real difference. A developer pasting code into an approved AI tool to fix a bug is doing their job. Someone pasting the same code into a personal AI account may be exposing the company's intellectual property. Ent can tell the difference and respond accordingly.

When something looks risky, Ent matches its response to the situation. An honest mistake may only need a helpful warning or a nudge toward an approved tool. A serious threat can be stopped before it does harm. When a case needs review, Ent provides a plain-language record that both security and business teams can understand. Ent also works alongside the security tools organizations already use.

Use cases for protecting human and AI work

People and AI agents rely on trusted access to get work done. That same access can expose sensitive information or give attackers a path into the business. Ent helps organizations manage these risks while keeping legitimate work moving. The following use cases show where that protection applies.

AI-powered threat prevention

Stops attacks that misuse trusted users and everyday tools before they can do damage.

AI & application control

Lets people and AI agents use approved AI tools safely, with guidance when they step outside company policy.

Insider risk prevention

Separates honest mistakes from serious risk and helps teams act earlier with clear evidence. One customer built an insider-risk program from scratch and delivered more than $5M in net impact within nine months.

Endpoint data protection

Protects sensitive information wherever it moves on the endpoint, including into AI tools, without blocking legitimate work.

Reduce risk while supporting productivity

With Ent, organizations can intervene before risky or malicious activity causes harm while allowing legitimate work to continue. Employees receive guidance when an action creates risk so they can make a safer choice without having an entire application blocked. Security teams gain a connected view of what happened and the context to decide what needs attention. That helps them spend less time piecing together isolated events and more time addressing meaningful risk.

Ent also helps organizations adopt AI with greater confidence. According to Gartner, more than 57% of employees use personal AI accounts for work and 33% admit to entering sensitive information into unapproved tools. Ent helps teams establish boundaries for how people and agents use AI and handle sensitive information. When activity crosses those boundaries, it can guide the user toward a safer action or stop the activity when needed. This supports AI adoption while reducing accidental exposure and reliance on unapproved tools.

These capabilities build on the security investments organizations already have. Ent adds context to investigations and can help consolidate selected legacy data protection and insider risk use cases alongside application control.

Source: Gartner Top Cybersecurity Trends for 2026

Protect work as it happens

See Ent in action

Schedule a demo to learn how Ent helps protect human and AI-driven work before risk becomes an incident. See how it connects everyday actions to recognize risk and applies a response that fits the situation.

We'll walk through scenarios relevant to your organization and show how Ent supports safer AI adoption without slowing legitimate work. You'll also learn how it fits alongside your existing security tools and where to begin based on your priorities.

Learn more at ent.ai.

About Ent

Ent® is an AI endpoint security company for human and agentic work. Ent uses AI on the endpoint to understand human and agent activity in sequence and the intent behind it, then applies programmable policy and inline controls before risky or malicious activity becomes an incident.

By combining first-party endpoint telemetry, behavioral intelligence, local AI reasoning, and deterministic controls, Ent protects execution, data, and work through one endpoint context and enforcement layer. Ent was founded by Elias Manousos and Brandon Dixon and works with enterprises across financial services, hospitality, defense, and other security-sensitive industries.