Protect work as it happens

Stop risky actions before they become incidents

AI has changed how work happens. People and AI agents use trusted applications to access information and take action across the endpoint. Agents can work with a user's credentials and move faster than a person can review each step. Meanwhile, attackers exploit trusted tools and manipulate workflows to advance their attacks. Individual actions may appear legitimate even when the sequence creates risk.

Ent is intent-aware AI endpoint security for human and agentic work. The Ent Intent-Aware Endpoint Platform connects activity in sequence to understand what is happening and why. It applies programmable runtime policy and inline controls before risky or malicious activity becomes an incident.

What Ent protects against

Ent evaluates activity against organizational policy and expected behavior. Local AI reasoning helps interpret the surrounding context so the response matches the risk and legitimate work can continue.

Threat Prevention for AI-Powered Attacks
Recognize when legitimate-looking actions form a malicious sequence. Intervene before attacks that manipulate users or abuse trusted tools can complete.

AI & Application Control
Understand which applications and AI agents are running and what they are doing. Control execution across tools and scripts when activity moves outside approved policy.

Insider Risk Prevention
Distinguish legitimate work from mistakes or malicious activity. Identify externally directed behavior and risky agent actions while preserving the sequence for investigation.

Endpoint Data Protection
Protect sensitive data across applications and AI interactions, including browser and clipboard workflows. Guide users toward safer actions or redact sensitive information before exposure. Block the action when needed.

What customers achieve with Ent

Organizations can enable AI adoption while maintaining control over sensitive work. Proportionate interventions help users correct course and stop harmful actions without defaulting to blanket application blocks.

When investigation is needed, connected evidence helps teams understand what happened and why. Ent complements existing endpoint security and enriches security operations workflows. It can also consolidate selected legacy DLP and insider-risk/UEBA use cases as well as application control.

See Ent in action

Schedule a demo to learn how Ent understands human and agentic work and applies the right controls before risk becomes an incident.

Visit ent.ai/contact

Why intent makes the difference

Sequence-level intent
Connect first-party endpoint telemetry across human and agent activity to understand how actions relate and when they create risk.

Programmable runtime policy
Turn organizational policy into controls that account for the actor and the work. Validate policies against historical activity before enforcement.

Inline prevention
Combine local AI reasoning with deterministic controls to apply decisions where actions happen, while there is still time to prevent impact.

Data sovereignty
Support customer requirements for sensitive telemetry and processing through local reasoning and SaaS or customer-controlled deployment options.

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.