Cybersecurity
Progress. Protected.

Reduce risk, not innovation with ESET AI Security

The problem

AI tools and autonomous agents are rapidly becoming part of everyday business operations. As they integrate into workflows and interact with external content, they introduce new pathways by which threats can reach your organization.

While the risks themselves are not always new, the way they appear is changing—through AI-generated outputs, automated actions, and user interactions, which can create AI blind spots for security and compliance teams.

The solution

ESET AI SECURITY

AI Security is a dedicated layer of protection designed to secure the ways in which AI is used across your organization. It focuses on the real points of exposure—where AI tools, agents, and users interact with data, systems, and external content.

HOW IT WORKS

Early detection of suspicious activity

We flag behavior that may indicate risk before it escalates into a security incident

Monitoring of AI-driven behavior

We track how AI tools and agents operate on endpoints to identify unusual or unexpected activity

Clear visibility into AI activity

We provide insight into how AI is behaving, helping your teams understand and investigate risks faster

Integrated incident reporting and response

AI Security automatically creates incidents in ESET PROTECT for streamlined investigation and action

Benefits of ESET AI Security

BUILT INTO YOUR EXISTING SECURITY

AI Security is integrated directly into ESET endpoint protection, extending your coverage without adding complexity or new tools.

REAL-TIME PROTECTION WHEREVER AI OPERATES

Security controls are applied where AI activity happens—across endpoints, user interactions, and automated processes.

ENABLING SAFE AI ADOPTION

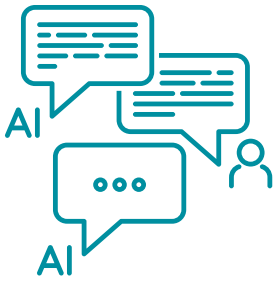
With ESET, your organization can adopt AI confidently—reducing risk without restricting productivity or innovation.

DATASHEET

ESET AI Security

AI is a new, distinct attack surface that is becoming part of every workflow and every application, across home users and organizations. Securing those workflows and applications requires an AI-native security architecture that can protect them—and the AI supply chain.

Protect yourself against modern AI-enabled threats with these new ESET AI Security modules:



AI CONVERSATION SECURITY

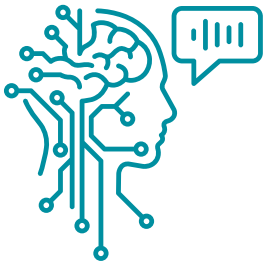
AI Conversation Security adds browser-based protection for interactions between users and LLMs

Scans URLs in LLM responses

Scans scripts generated by LLMs to prevent malicious code execution

Flags sensitive data (private keys, access tokens, etc.) in users' prompts to prevent data leakage

Checks uploaded files and their metadata for sensitive content tags



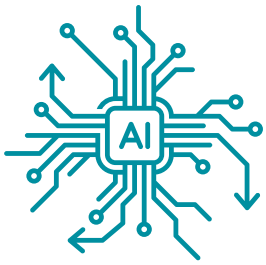
AI AGENT SECURITY

AI Agent Security adds a dedicated layer of protection within endpoint security to target threats entering through the AI ecosystem.

Prevents AI agents from accessing and downloading malicious agents across the AI supply chain

Scans AI files, components, URLs, and download chains to stop multistage attacks

Allows organizations to adopt autonomous agents without opening new security gaps



AI BEHAVIORAL MONITORING

AI Behavioral Monitoring adds visibility for autonomous AI agents, focusing on autonomous AI agent behavior and actions

Stops potential threats by identifying suspicious AI agent behavior

Suspicious AI agent activities are flagged and marked as incidents for investigation

DATASHEET

CONTACT US

ESET North America
1 (844) 824-3738

www.eset.com