so why Ermes

Proactive AI-Driven Protection for Browsers
Detects and blocks threats in real time, beyond static threat intelligence or reputation lists.

Lightweight, Fast Deployment
Delivered via browser extension — no infrastructure changes needed, full rollout typically in couple hours.

Seamless Integration with Existing Security Stack
Sends enriched, actionable browser session logs directly into SIEM, XDR, and MDR platforms.

Complements EDR, XDR, MDR — No Overlap
Protects where existing tools lack visibility, the browser layer.

Maximizes Existing Security Investments
Adds unique, detailed browser session intelligence to strengthen the performance of existing security tools.

Built-in Services for Effortless Adoption
Includes Customer Success and expert services within the license to help teams get the most out of Ermes, reducing the workload on internal security staff.

Zero infrastructures

Easy to deploy

Invisible for the user

On device protection

Gartner
TOP 10 Browser Security vendor

Below you can find the companies and partners who decided to trusts us over this amazing journey

MAIRE
TIM
Carrefour
KPMG
IBSA
FAAC
SOLGROUP a breath of life
Romagna Acque Società delle Fonti
DUMAREY
TIGROS
BonelliErede
BALOCCO
GRUPPO CREMONINI
CHIOMENTI
Fratelli Beretta 1812
ALFAGOMMA
Aeroporto di Bologna
LA7
ABS
F2i
AirDolomiti
Cuki
facile.it
GRUPPO MONTENEGRO
urmet
sorgenia
IVECO DEFENCE VEHICLES
BANOR
Marchesi ANTINORI
DISARONNO ORIGINALE

ERMES
BROWSER SECURITY

Your Business Runs on the Browser.

Browsers are representing more and more the Operating Systems of the future.

90% of cyber-attacks happen via Browsers, and DORA, NIS2, and GDPR are increasing pressure on this sector.

We Make Browsers Enterprise.

Do you want to be one of the potential attacking targets?

Ermes Browser Security is here to help you with its groundbreaking technology to make the browser your employees use during their daily working activities enterprise.

Ermes is the unique vendor in Europe and Italy recognized by Gartner as a global **Top 10 browser security solutions.**

With its browser-native architecture and proprietary AI technology, it offers **a complete suite for enterprises** → to be protected against cyber-attacks originating from browser use.

AI Based Protection

Zero-Day Phishing Protection:
a proprietary AI engine detects and blocks newly registered malicious hostnames and domains that 40% of the times remain unidentified by other CTI sources, within 24 hours.

Real Time Protection:
an in-browser Deep Learning that detects threats like 0-day phishing implementing detection evasion techniques (e.g., CAPTCHA cloaking) in real time, instantly alerting end-users and blocking phishing attacks.

Cybersquatting & Malicious URL Protection:
shields users from misleading or harmful hostnames and domains using AI models and proprietary threat intelligence.

Malvertising & Tracking Protection:
eliminates invasive ads, trackers, and cryptominers, while reducing noise in security logs.

SESSION Protection

Web Data Loss Prevention (DLP):
prevents data exfiltration via copy, paste, upload operations, PII and keyword/patterns with both audit and blocking modes.

Business Credentials Protection:
stops unauthorized use of corporate credentials on unapproved apps and domains.

Browser Extensions Protection:
identifies and analyzes extensions installed by users, evaluating malicious traits, execution behavior, permissions, known vulnerabilities in dependencies, reputation, and presence on official stores.

Browsing Risk Assessment:
classifies navigation risk in real time, with native SIEM/SOAR integration.

Advanced Web Filtering:
provides fine-grained URL filtering without relying on VPNs or SSL inspection, ensuring performance and user privacy.

Contextual DLP

Ermes Contextual DLP leverages AI and LLMs to understand data in context.
It prevents leaks by blocking or masking sensitive information before it leaves the browser.
Users receive real-time guidance to distinguish what can and cannot be shared.
This ensures compliance, awareness, and protection without disrupting productivity.