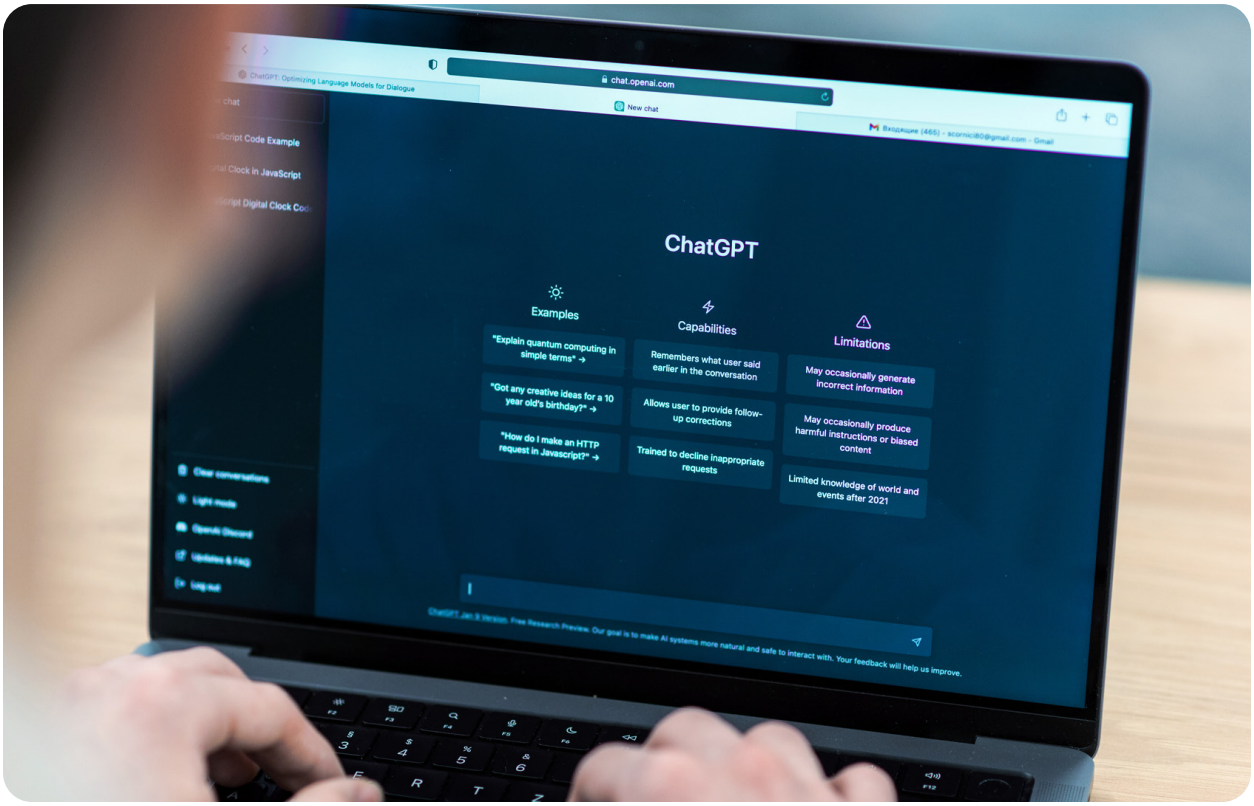
MAMMOTH CYBER

Mammoth Enterprise Browser: Zero Trust on Zero Day for LLM-Centric AI

Overview

Mammoth Enterprise Browser delivers Zero Trust on Zero Day, ensuring LLM security and AI security for enterprises.

This zero-trust browser combines advanced endpoint monitoring, granular policy enforcement, and real-time threat detection to protect Large Language Models (LLMs) and AI applications. It secures SaaS-based models (e.g., OpenAI, Anthropic, Google Gemini) and private models (e.g., Meta Llama, Amazon Bedrock) against emerging threats, ensuring compliance and data protection.



The Challenge

The rapid adoption of LLM-Centric AI introduces critical AI security risks, including prompt injection, unauthorized model access, shadow AI, and browser-related leaks, as outlined in the OWASP Top 10 for LLM applications. Enterprises face shadow AI proliferation, lack visibility into AI model usage, and struggle to prevent intellectual property (IP) exposure, sensitive data leaks, or compliance violations, especially in diverse environments with varying IT resources.

> **Enterprises face shadow AI, lack visibility into model usage, and struggle to prevent IP exposure and data leaks.**

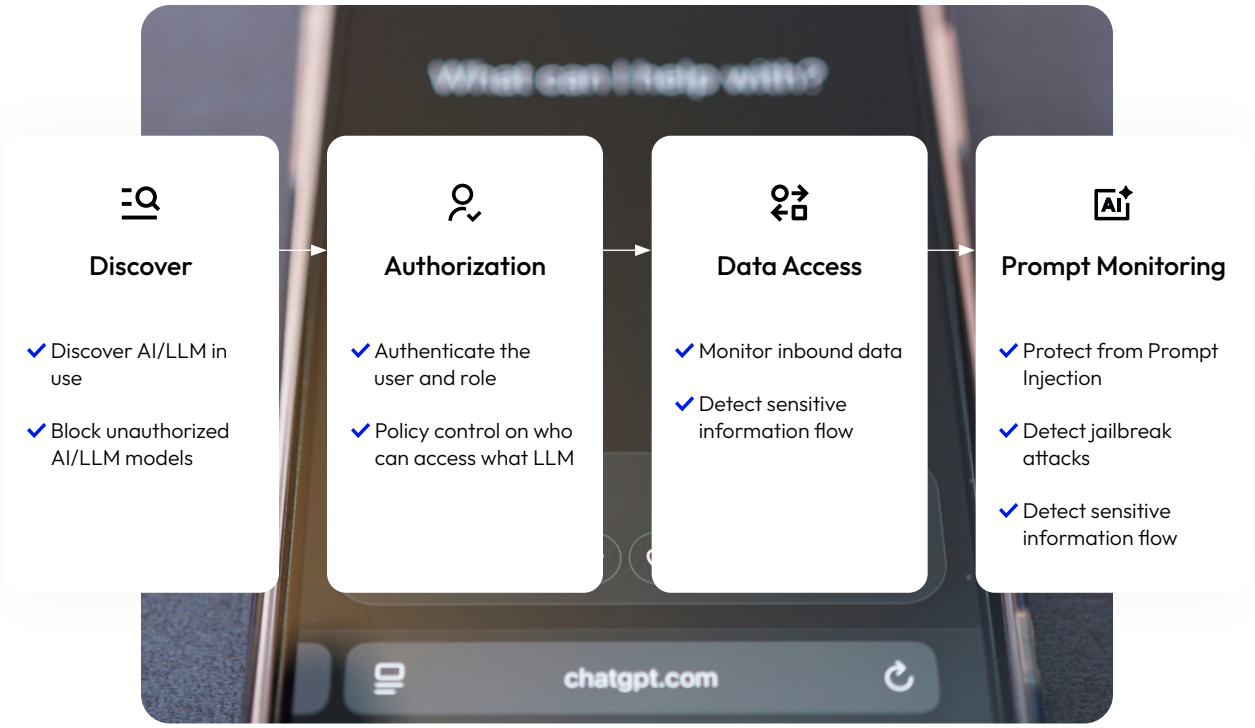
OWASP Top 10 LLM Risks

Risk	Description
LLM01 Prompt Injection	Crafty inputs manipulate LLMs, causing unintended actions.
LLM02 Insecure Output Handling	Unscrutinized LLM outputs expose systems to XSS or code execution via browsers.
LLM03 Training Data Poisoning	Tampered training data introduces vulnerabilities or biases.
LLM06 Sensitive Information Disclosure	LLMs reveal confidential data in browser responses, risking privacy breaches.
LLM07 Insecure Plugin Design	Insecure plugins allow exploitation, risking code execution.
LLM08 Excessive Agency	Overly autonomous LLMs perform unintended actions.
LLM09 Overreliance	Blind trust in LLMs leads to misinformation or legal issues.
LLM10 Model Theft	Unauthorized copying of LLMs causes economic losses.
Supply Chain Vulnerabilities	Weak components or datasets introduce security risks.
Model Denial of Service	Resource-heavy operations degrade service or increase costs.

Mammoth's Solution

Mammoth Enterprise Browser delivers Zero Trust on Zero Day by securing LLM-Centric AI against AI security risks and browser-related leaks.

Combating Shadow AI: Shadow AI—unauthorized use of AI models like unapproved SaaS-based LLMs or generative AI tools—poses significant risks, including data leakage and compliance violations (LLM08, LLM10). Mammoth Enterprise Browser addresses this by discovering all LLM-Centric AI instances across browsers and endpoints, using real-time monitoring to detect rogue applications. It enforces strict policies to block unauthorized models, integrates with identity providers for user verification, and provides detailed audit logs to ensure governance, empowering organizations to eliminate shadow AI risks while maintaining productivity.



Additional technical capabilities include:

Shadow AI Detection	Identifies unauthorized AI models and agents, preventing shadow AI usage (LLM08, LLM10).
User Authorization	Integrates with identity providers (e.g., Okta, Azure AD) for role-based access control, ensuring only authorized users interact with LLMs (LLM07, LLM09, LLM10).

Prompt Injection Protection	Monitors prompt inputs to block prompt injection attacks and jailbreak attempts, leveraging Virtue AI for advanced detection (LLM01).
Data Leakage Prevention	Inspects prompt inputs/outputs to prevent leaks of PII, source code, or IP, with inline data classification (LLM02, LLM06).
Compliance Monitoring	Detects non-compliant outputs (e.g., violent or sensitive content) and generates audit logs for governance, integrating with SIEM tools like Splunk for real-time analytics (LLM06).
API & Network Security	Deploys a local proxy to monitor AI API calls, detecting malicious network activities and securing integrations (LLM07, LLM10).
AI Guardian	Provides AI-based phishing protection and monitors for LLM-specific threats like prompt pollution.

Benefits

Proactive Security

Mitigates OWASP LLM risks like prompt injection, shadow AI, and browser-related leaks with real-time defenses.

Comprehensive Visibility

Enables AI governance through detailed AI model monitoring and SIEM integration.

Regulatory Compliance

Ensures data security with robust audit trails.

Enhanced Productivity

Balances secure AI access with seamless usability for diverse workforces.

Cost Efficiency

Replaces complex security stacks with a scalable enterprise browser.

Why Mammoth Cyber?

Founded in 2019 by cybersecurity experts, Mammoth Cyber is a leader in enterprise browser security. Mammoth Enterprise Browser is widely adopted by organizations ranging from those with legacy mission-critical private apps and limited IT staff to large distributed banking organizations with remote workers and multiple offices. Backed by the trust of industry-wide security and IT practitioners, it addresses OWASP LLM risks with innovative AI security solutions. Strategic partnerships, including Virtue AI, ensure continuous advancements in LLM protection.

> **"Mammoth Enterprise Browser eliminated browser-related leaks and shadow AI risks for our legacy apps."**
>
> IT MANAGER, MANUFACTURING FIRM

> **"Prompt injection protection and SIEM integration transformed our distributed banking operations."**
>
> CISO, GLOBAL BANK

MAMMOTH CYBER

Schedule a self-start from your mobile device at **mammothcyber.com** or contact **demo@mammothcyber.com** to secure your LLM-Centric AI with Zero Trust on Zero Day!

Get Started