SOLUTION BRIEF

AI Security Starts at the Endpoint: Safeguarding Generative AI Powered Solutions

Generative AI: Transforming the Security Landscape

Generative AI is reshaping software from the ground up, turning it into a dynamic, intelligent service that learns, adapts, and creates in real time. Large Language Models (LLMs) and Generative AI are redefining software by acting as core components rather than add-ons, empowering real-time interactions that anticipate and evolve with user needs. Traditional security simply cannot keep pace with this transformation.

Why Now? As generative AI rapidly integrates into business environments, security frameworks must evolve in real time. The threat of prompt-based attacks, like prompt injection, introduces vulnerabilities that traditional cloud and network-based security cannot address. Endpoint AI Security is no longer optional—it is essential for ensuring that businesses harness AI's potential safely, guarding sensitive data from emerging threats.

Challenges

1. **Dynamic AI Interactions**
   Traditional security models cannot keep up with AI's evolving and contextual nature, creating vulnerabilities in common user interactions.
2. **Unfettered AI Access**
   New AI models are popping up every week. Preventing access to unauthorized AI SaaS services can be a major hurdle.
3. **Limits of Existing Security Models (SASE):**
   Securing AI interactions with a cloud-based solution introduces latency that can kill user productivity.

Endpoint AI Security: Protecting the Prompt in Real-Time

Endpoint AI Security provides real-time protection by securing interactions at their source, specifically focusing on safeguarding the prompt as the key input to AI models. By intercepting potential threats directly at the device level, this approach ensures that AI behavior remains aligned with intended usage.

Deployed through an Enterprise Browser, this solution incorporates multiple layers of security: it monitors and sanitizes prompts to prevent malicious commands, safeguards every user-AI interaction at the endpoint to block threats from reaching the AI model, and integrates continuous monitoring to detect and respond to suspicious activities, thus maintaining compliance and security.

Key Benefits and Differentiators:

1. **Immediate Threat Mitigation:** Prompt security at the endpoint blocks malicious inputs before they reach the cloud.
2. **Enhanced User Experience:** Minimizes latency for real-time applications by securing AI interactions locally.
3. **Controlled AI Access:** Enterprise Browsers enforce usage of only secure, authorized AI models, preventing unauthorized or insecure AI interactions.

Implementing Endpoint AI Security with the Mammoth Cyber Enterprise Browser

Aligned with OWASP AI security guidelines, the Mammoth Cyber Enterprise Browser enforces strict security controls, including multi-factor authentication, role-based access control, and continuous monitoring to ensure only authorized users and devices interact with the AI model. It also isolates AI interactions within a secure environment, creating a safe place that prevents data cross-contamination. Furthermore, its Prompt Guard feature analyzes and filters prompts for policy violations, effectively blocking AI outputs from disclosing sensitive or unauthorized information.

Endpoint AI Security is foundational for secure, innovative AI-driven applications. By implementing prompt protection at the endpoint, enterprises can safely leverage the power of generative AI, aligning security with the evolving landscape of software services.

The Mammoth Difference

Our Mammoth Enterprise Browser solution solves critical access problems while protecting data, improving security posture, driving compliance, accelerating deployment and simplifying policy management.

- Prevent data theft with control over the access and actions of employees, 3rd party contractors and partners
- Enhance productivity and increase adoption with a seamless end user experience and simple deployment
- Enable the shift to a zero-trust security architecture with visibility and control at a critical access point
- Drive compliance to industry mandates with visibility and audit logs for user behavior

Schedule a Demo

+1 669 699 1122 | info@mammothcyber.com

MAMMOTH CYBER