CLOUDFLARE

เร่งการนำเทคโนโลยี AI มาใช้ด้วยการออกแบบที่คำนึงถึงความปลอดภัย

AI ได้เข้ามามีบทบาทอย่างเต็มที่แล้ว ขณะที่ระบบความปลอดภัยแบบดั้งเดิมไม่อาจก้าวทันการเปลี่ยนแปลง

98%

ขององค์กรมีการใช้งานแอปพลิเคชันที่ไม่ได้รับอนุญาต รวมถึง Shadow AI ช่องว่างเหล่านี้ก่อให้เกิดความเสี่ยงต่อการรั่วไหลของข้อมูลและการละเมิดข้อกำหนด[1]

50%

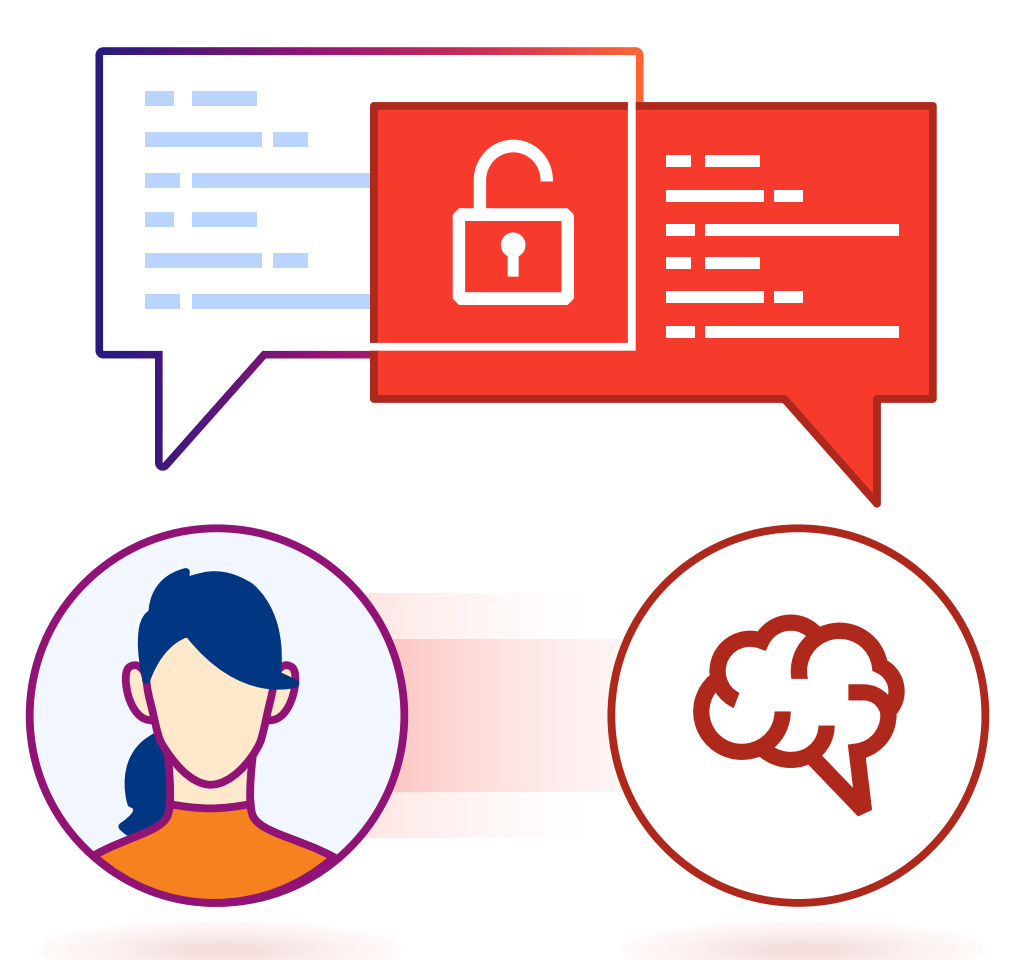
การโจมตีด้วยวิธี Prompt Injection มีอัตราความสำเร็จ 50% และถูกจัดให้เป็นภัยคุกคามด้านความปลอดภัยอันดับต้นในรายชื่อ OWASP Top 10 สำหรับแอปพลิเคชันที่ใช้โมเดลภาษา LLM[2]

97%

ขององค์กรที่ประสบเหตุด้านความปลอดภัยซึ่งเกี่ยวข้องกับ AI ไม่มีระบบควบคุมการเข้าถึง AI ที่เหมาะสม[3]

93%

ของพนักงานยอมรับว่าได้ป้อนข้อมูลเข้าสู่เครื่องมือ AI โดยไม่ได้รับอนุญาต[4]



ปกป้องวงจรการทำงานของ AI ด้วย Cloudflare

ครอบคลุมทั้ง Generative AI และ Agentic AI

ความปลอดภัยระหว่างมนุษย์กับ AI

บุคลากรของคุณ

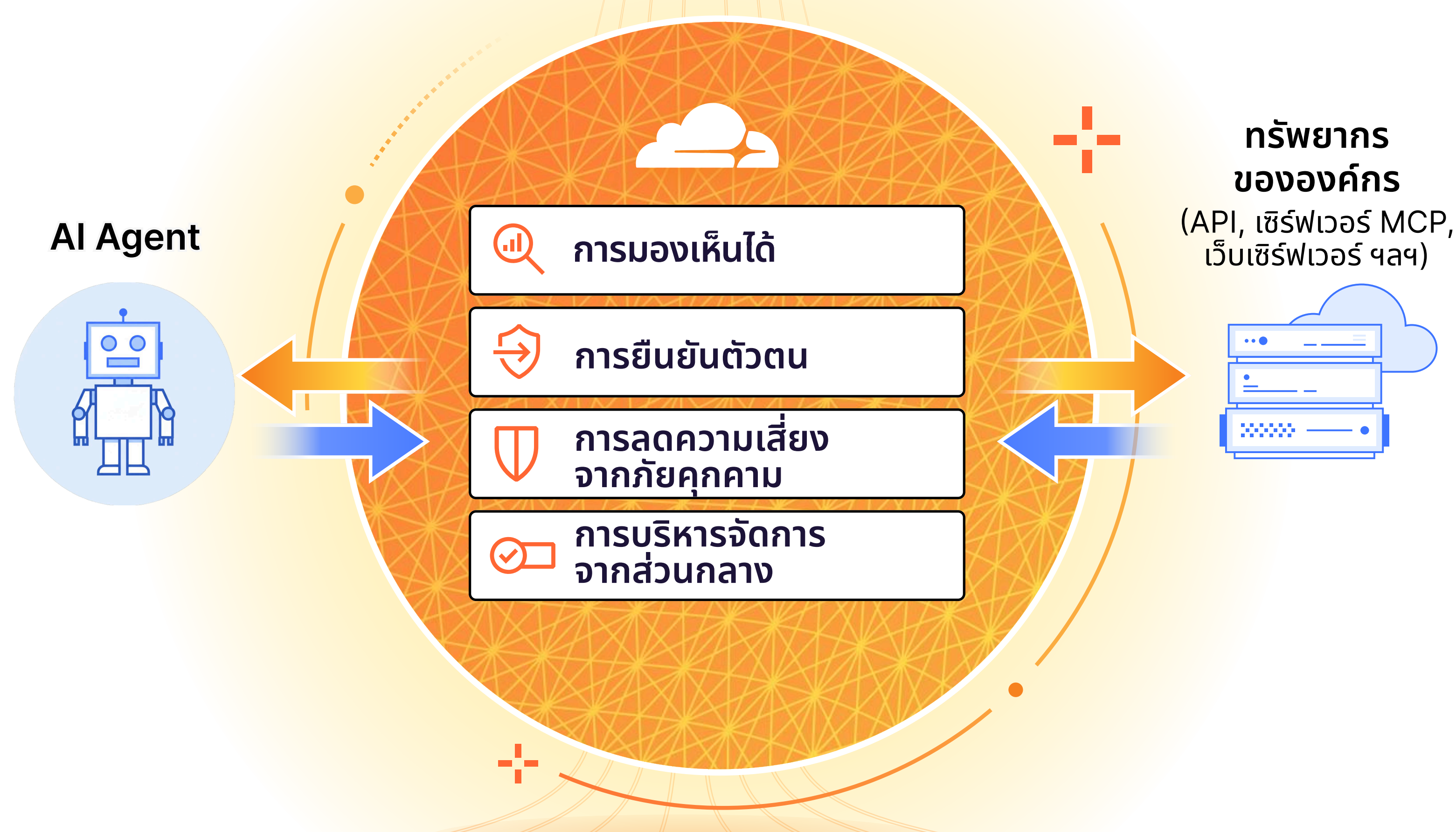
ลูกค้าของคุณ

- การค้นพบ
- การควบคุมการใช้งาน
- ความปลอดภัยของข้อมูล
- การลดความเสี่ยงจากภัยคุกคาม
- การบริหารจัดการจากส่วนกลาง

แอปพลิเคชัน AI แบบสาธารณะหรือแบบภายในองค์กร (สำหรับพนักงานของคุณ)

แอปพลิเคชันที่ขับเคลื่อนด้วย AI (สำหรับลูกค้าของคุณ)

ความปลอดภัยของ Agentic AI



AI Agent

- การมองเห็นได้
- การยืนยันตัวตน
- การลดความเสี่ยงจากภัยคุกคาม
- การบริหารจัดการจากส่วนกลาง

ทรัพยากรขององค์กร (API, เซิร์ฟเวอร์ MCP, เว็บเซิร์ฟเวอร์ ฯลฯ)

ขยายขอบเขตการมองเห็น

ครอบคลุมทั้งแอปพลิเคชัน AI อุปกรณ์ปลายทาง API และการเชื่อมต่อระหว่าง AI Agent และ MCP

จัดการความเสี่ยง

ด้วยกลไกป้องกัน การควบคุมสถานะความปลอดภัย และการลดความเสี่ยงจากภัยคุกคามแบบเรียลไทม์

ปกป้องข้อมูล

พร้อมด้วยการป้องกันพรอมต์และการควบคุมการเข้าถึงสำหรับพนักงานและ AI Agent

มีระบบความปลอดภัยในตัวตั้งแต่ต้น

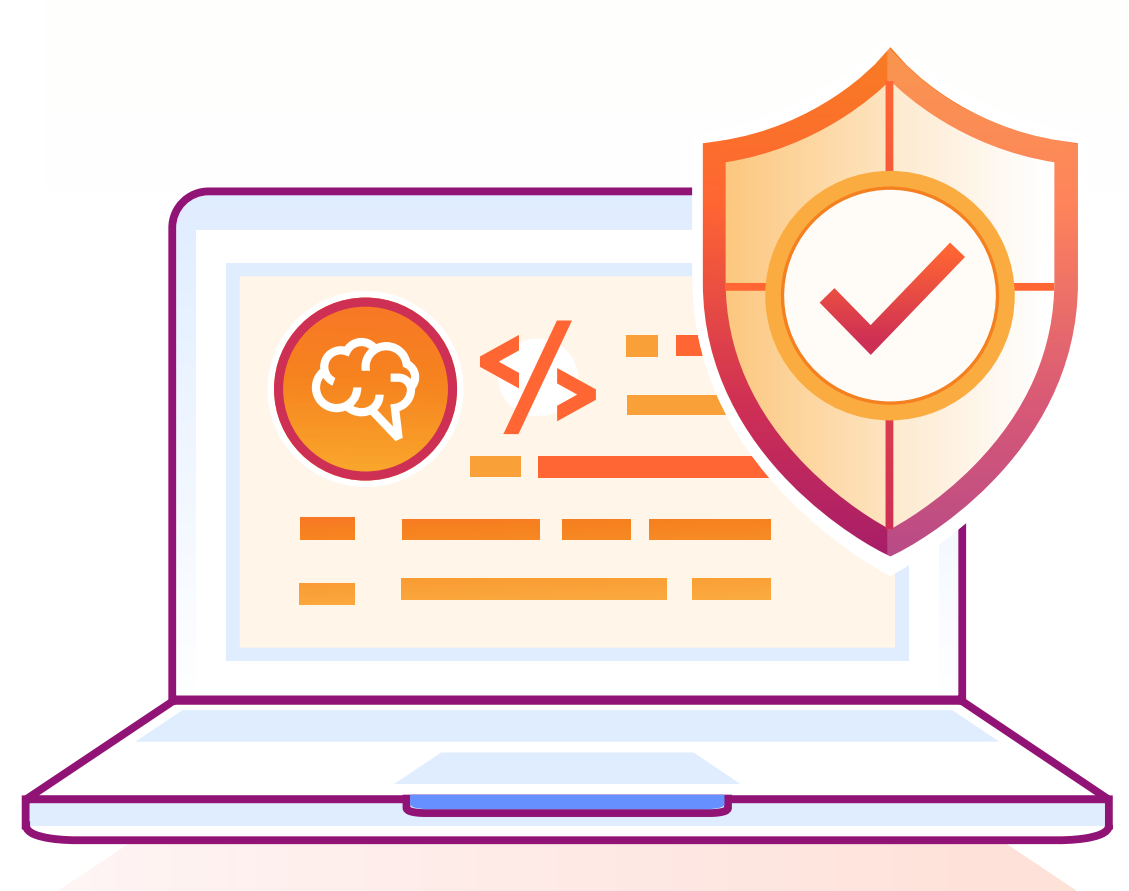
เมื่อพัฒนา AI บนแพลตฟอร์ม Cloudflare

ทำให้การใช้งาน GenAI ของบุคลากรมีความปลอดภัย

- ค้นพบการใช้งาน Shadow AI
- ประเมินความเสี่ยงของแอปพลิเคชัน AI
- จัดการสถานะความปลอดภัยของแอปพลิเคชัน AI
- จำกัดการป้อนข้อมูลที่มีความอ่อนไหว
- บังคับใช้กลไกป้องกันในพรอมต์และการตอบกลับ

ปกป้องแอปพลิเคชันและเวิร์กโหลดที่ขับเคลื่อนด้วย AI

- ตรวจพบจุดเชื่อมต่อของ Shadow AI
- ปกป้องโมเดล AI และข้อมูลฝึกสอนจากการใช้งานในทางที่ผิด
- ป้องกันไม่ให้ข้อมูลระบุตัวบุคคล (PII) รั่วไหลในคำสั่งพรอมต์และการตอบกลับ
- บังคับใช้การกลั่นกรองเนื้อหา



ทำให้สิ่งที่คุณสร้างขึ้นมีความปลอดภัย

- สร้างเซิร์ฟเวอร์ MCP ที่มีระบบการยืนยันตัวตนและการกำหนดสิทธิ์ในตัว
- บันทึกและจำกัดคำขอ/การตอบกลับของโมเดล AI รวมถึงการใช้โทเค็นและต้นทุนที่เกิดขึ้น
- ป้องกันการหยุดชะงักของบริการด้วยกลไกสำรองของโมเดลและการจำกัดอัตราการเรียกใช้งาน

Cloudflare สร้างความแตกต่าง

การปกป้องวงจรชีวิตของ AI อย่างครอบคลุม

แพลตฟอร์มเดียวที่ช่วยรักษาความปลอดภัยในการสื่อสารระหว่างมนุษย์กับ AI และระหว่าง AI กับทรัพยากร ตั้งแต่ขั้นตอนการพัฒนาไปจนถึงการนำไปใช้งานจริง

ระบบความปลอดภัยของ AI แบบเรียลไทม์ที่ทำงานอินไลน์

รักษาความปลอดภัยของพรอมต์และการตอบกลับของ AI แบบเรียลไทม์ ด้วยการควบคุมที่ครอบคลุมทั้งสภาพแวดล้อม AI แบบสาธารณะและแบบภายในองค์กร

สถาปัตยกรรม AI ระดับโลกที่รองรับการพัฒนาในอนาคต

ใช้ประโยชน์จากเครือข่ายระดับโลกของเราเพื่อการบังคับใช้ที่ระดับขอบเครือข่ายอย่างต่อเนื่อง พร้อมรองรับขนาดและสมรรถนะที่ AI ต้องการ

การปรับใช้แบบไม่ขึ้นอยู่กับโมเดล

กลไกควบคุมด้านความปลอดภัยสามารถทำงานร่วมกับโมเดล AI ทุกประเภทในสภาพแวดล้อมของคุณ โดยมอบแนวทางแบบรวมศูนย์เพื่อการกำกับดูแลการปรับใช้ AI

กรณีศึกษาจากลูกค้า

indeed

เว็บไซต์หางานอันดับ 1 ของโลก

ระบุและควบคุมการใช้งาน Shadow AI

ดำเนินการควบคู่ไปกับโครงการปรับปรุงระบบการเข้าถึงระยะไกลให้ทันสมัย

บริษัท SaaS ที่ใช้ AI

ปกป้องข้อมูลระบุตัวบุคคล (PII)

โดยป้องกันไม่ให้ลูกค้าส่งข้อมูลที่มีความอ่อนไหวไปยังจุดเชื่อมต่อของ GenAI ที่เปิดให้เข้าถึงจากภายนอก

Cyndx

บริษัทฟินเทคที่ขับเคลื่อนด้วย AI

ลดต้นทุนการประมวลผลแบบอนุมานได้ถึง 95%

โดยการนำ Cloudflare มาใช้ในการแคชและประมวลผลการตอบกลับจากผู้ให้บริการโมเดล AI

ค้นพบว่า Cloudflare สามารถช่วยรักษาความปลอดภัยให้กับการนำ AI าใช้งานของคุณได้อย่างไร

สำรวจกรณีการใช้งาน

---

1. Varonis, 2025 State of Data Security
2. Liu, S., Wang, Z., Chen, Y., Deng, G., Liu, Y., & Liu, Y. (2024). Automatic and Universal Prompt Injection Attacks against Large Language Models
3. IBM, 2025 Cost of a Data Breach
4. ManageEngine, The Shadow AI Surge in Enterprises

1 888 99 FLARE | enterprise@cloudflare.com | Cloudflare.com

REV:BDES-8274.2025OCT13

CLOUDFLARE