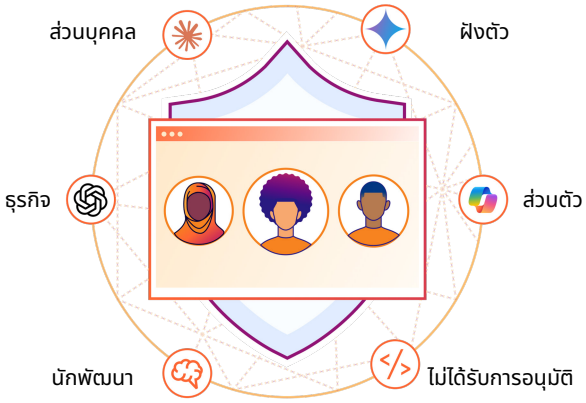
การใช้ generative AI และ agentic AI อย่างปลอดภัยภายในกลุ่มพนักงาน

เสริมพลังให้ทีมของคุณสามารถใช้เครื่องมือ AI ใด ๆ ก็ได้อย่างปลอดภัย พร้อมการป้องกันที่บังคับใช้โดยแพลตฟอร์ม SASE ของ Cloudflare



คืนการควบคุมพร้อมปลดล็อกประสิทธิภาพการทำงาน

การเร่งรีบนำ AI มาใช้ทำให้เกิดความเสี่ยงที่เพิ่มขึ้นมากมาย รวมถึงการรั่วไหลของข้อมูล การละเมิดกฎระเบียบ และพื้นที่การโจมตีที่ขยายตัว การปิดกั้น AI โดยตรงจะจำกัดความสามารถในการแข่งขันของคุณเท่านั้น และการทดลองผ่านโซลูชันเฉพาะจุดจะเพิ่มความซับซ้อนให้กับคุณเท่านั้น

Cloudflare ช่วยปกป้องการใช้ AI ขององค์กรของคุณโดยขยายความสามารถในการมองเห็น บรรเทาความเสี่ยง และปกป้องข้อมูลอย่างครอบคลุมในสภาพแวดล้อม AI:

- **สำรวจ shadow AI** และจัดการนโยบายสำหรับเครื่องมือ AI ที่ได้รับอนุมัติและไม่ได้รับอนุมัติทั้งหมด
- **เพิ่มความแข็งแกร่งในการกำกับดูแล AI** ด้วยการควบคุมการเข้าถึงที่อิงตามข้อมูลประจำตัวและการจัดการสถานะ
- **หยุดยั้งการสูญเสียข้อมูล** ด้วยการบล็อกข้อมูลที่ละเอียดอ่อนใน prompts ของผู้ใช้ บังคับใช้มาตรการป้องกันตามหัวข้อ และสแกนหาการกำหนดค่าที่ไม่ถูกต้องในเครื่องมือ AI

ขยาย Cloudflare เพื่อนำ AI มาใช้อย่างปลอดภัย ไม่ว่ากลยุทธ์ AI ของคุณจะเกี่ยวข้องกับการจำกัดการใช้งานแอปพลิเคชันเฉพาะหรือการทดลองใช้เครื่องมือที่หลากหลายมากขึ้นก็ตาม

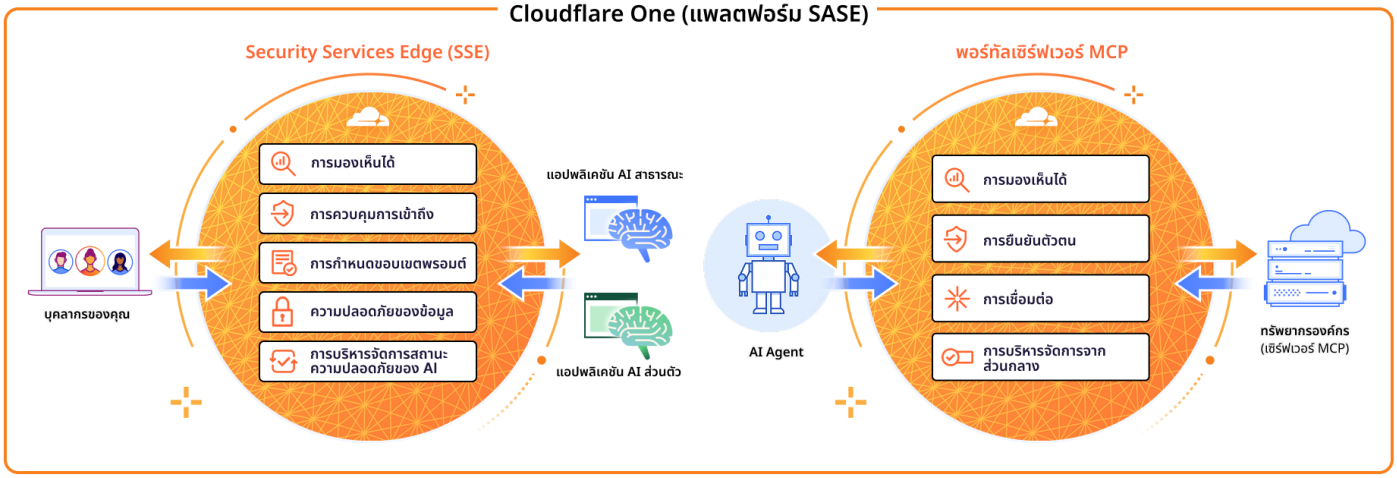
เหตุใด SASE จึงควรรักษาความปลอดภัยของการใช้ AI ภายในกลุ่มพนักงาน

แพลตฟอร์ม Service Edge สำหรับการเข้าถึงที่ปลอดภัย (SASE) ของ Cloudflare อยู่ระหว่างพนักงานของคุณและเครื่องมือ AI ซึ่งทำให้ SASE กลายเป็นจุดเริ่มต้นที่เหมาะสมสำหรับหลาย ๆ คนที่ต้องการเริ่มใช้ AI อย่างปลอดภัย

ไม่ว่าพนักงานจะสนทนากับ ChatGPT หรือ AI agent กำลังรวบรวมข้อมูลจากทรัพยากรขององค์กร แพลตฟอร์ม SASE ของ Cloudflare ก็บังคับใช้การควบคุมความปลอดภัยที่สอดคล้องกัน

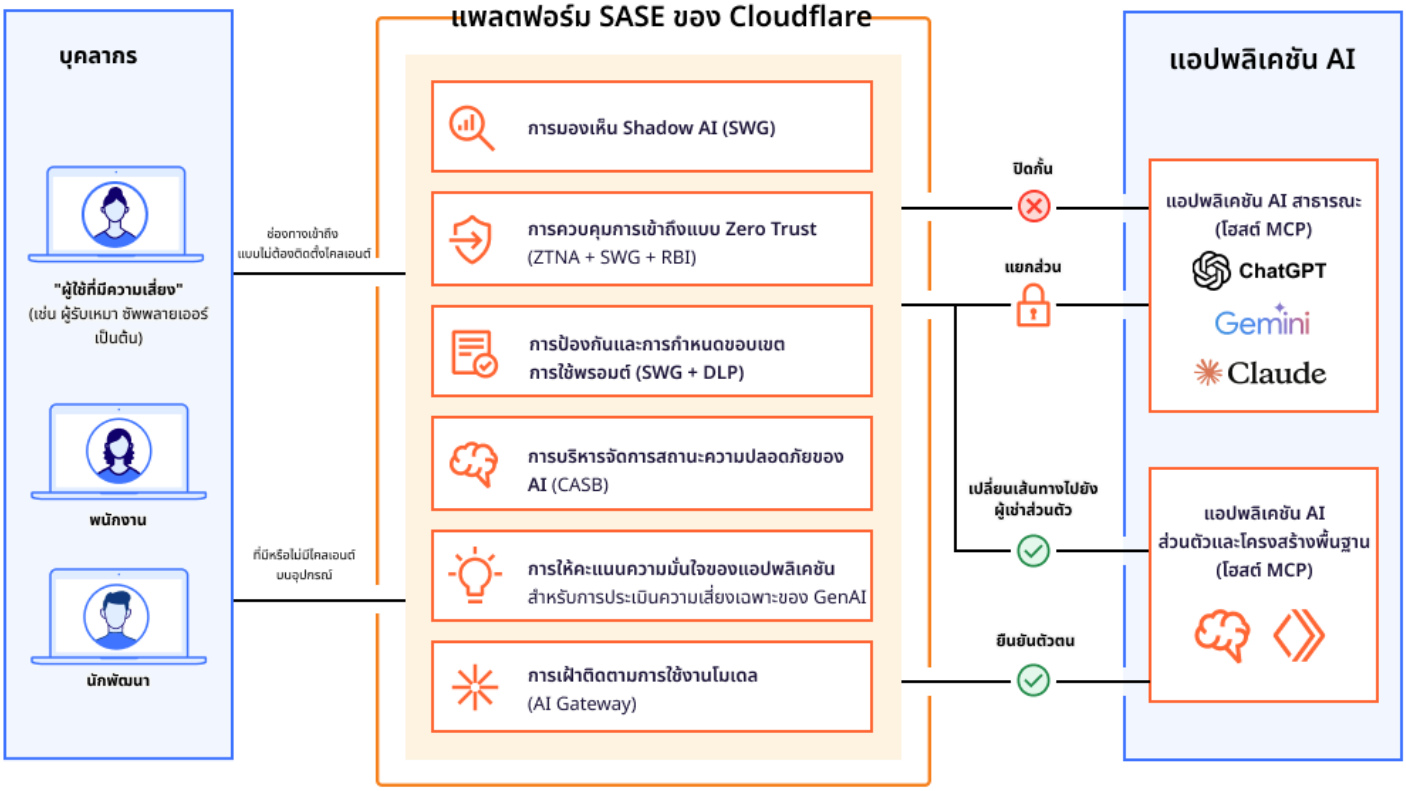
รักษาความปลอดภัยของ generative AI และ agentic AI

แพลตฟอร์ม SASE ของ Cloudflare มาพร้อมแดชบอร์ดรวมและระนาบการควบคุมเพื่อจัดการการโต้ตอบระหว่างมนุษย์กับ AI และระหว่างเครื่องกับเครื่องทั่วทั้งองค์กรของคุณ



Cloudflare ไม่เหมือนกับผู้จำหน่าย SASE รายอื่น ๆ เพราะ Cloudflare ยังช่วยเชื่อมต่อและปกป้องแอปและเวิร์กโหลดที่เปิดใช้งาน AI ที่เผยแพร่สู่สาธารณะ (เช่น แชทบอท AI ของเว็บไซต์ของคุณหรือเครื่องมือแนะนำ)

ปกป้องการสื่อสารของผู้ใช้ด้วยแอป generative AI
พร้อมการควบคุมการใช้งาน AI บนแพลตฟอร์ม SASE ของ Cloudflare



- **การมองเห็น:** ค้นพบและวิเคราะห์การใช้ shadow AI ผ่านการตรวจสอบทราฟฟิกแบบอินไลน์ ประเมินความเสี่ยงที่เกิดจากแอป AI เหล่านั้นด้วย การให้คะแนนที่โปร่งใส
- **การควบคุมการเข้าถึง:** บล็อก แยก เปลี่ยนเส้นทาง หรืออนุญาตการเชื่อมต่อของผู้ใช้ บังคับใช้กฎ Zero Trust ตามข้อมูลประจำตัวกับแอปแต่ละแอป
- **การป้องกันและการป้องกันที่รวดเร็ว:** ตรวจจับและบล็อก prompt ผู้ใช้ตาม เจตนา (เช่น ความพยายามเจลเบรก การใช้โค้ดในทางที่ผิด การร้องขอข้อมูลระบุตัวบุคคล)
- **ความปลอดภัยของข้อมูล:** หยุดการเปิดเผยข้อมูลที่ละเอียดอ่อนด้วยการตรวจจับ การป้องกันการสูญเสียข้อมูล (DLP) ที่ขับเคลื่อนด้วย AI สำหรับ PII, โค้ดต้นทาง และอื่น ๆ
- **การจัดการสถานะการรักษาความปลอดภัย AI:** รวมเข้ากับเครื่องมือ GenAI ผ่าน API (พร้อมใช้งานแล้วสำหรับ ChatGPT, Claude, Google Gemini) เพื่อสแกนหาการกำหนดค่าที่ผิดพลาดโดยใช้ Cloud Access Security Broker (CASB) ของเรา

ผลลัพธ์ของลูกค้า

indeed
เว็บไซต์หางานอันดับ 1 ของโลก

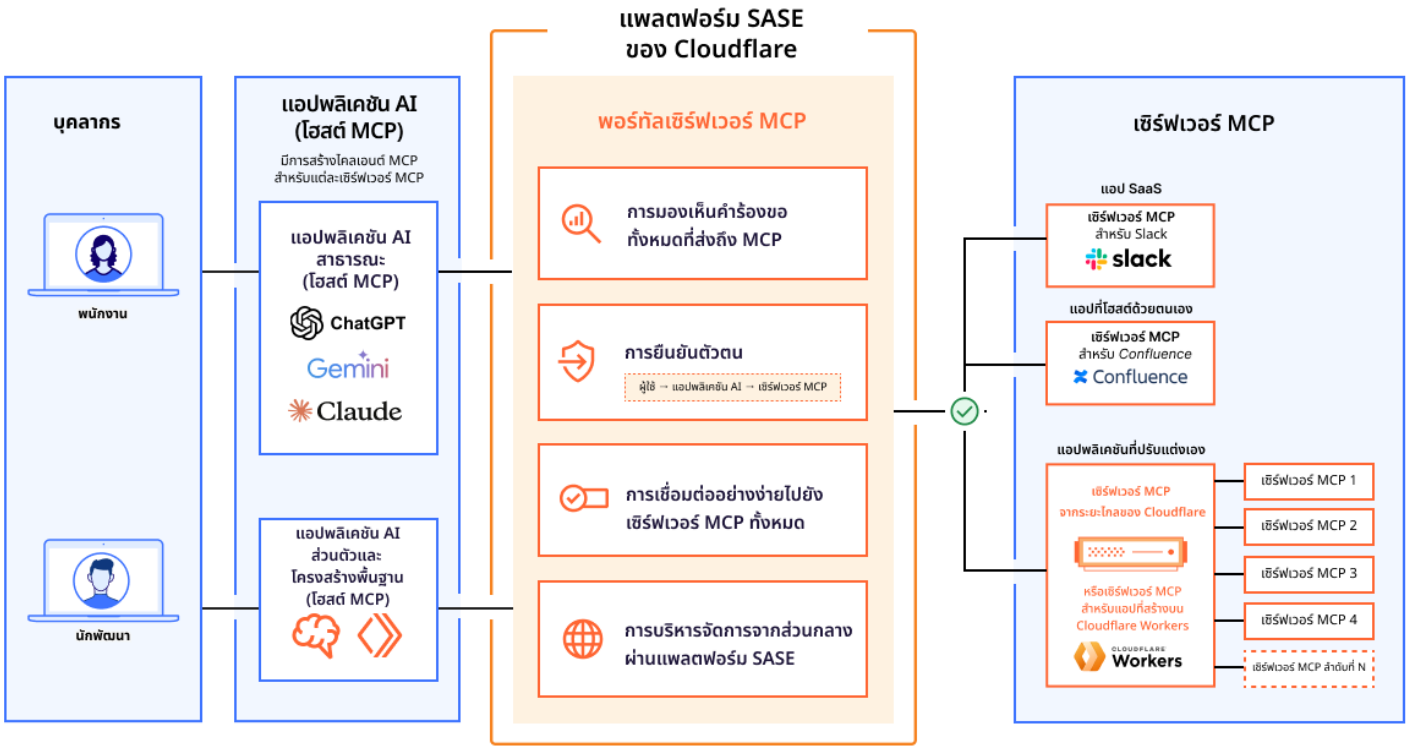
ระบุและควบคุม shadow AI ขนานไปกับโครงการเปลี่ยน VPN

APPLIED
เทคโนโลยีการประกันภัย

แยกเครื่องมือ GenAI สาธารณะ เช่น ChatGPT เพื่อปิดกั้นการคัดลอกและวางข้อมูลที่ละเอียดอ่อน

 02 026 0652 | enterprise@cloudflare.com | www.cloudflare.com

รักษาความปลอดภัยของการสื่อสารของ agentic AI (AI กับทรัพยากร)
ด้วยพอร์ทัลเซิร์ฟเวอร์ MCP บนแพลตฟอร์ม SASE ของ Cloudflare



- **การมองเห็น:** รวบรวมบันทึกคำขอ MCP ทั้งหมดเพื่อการตรวจสอบและวิเคราะห์ ตรวจสอบและอนุมัติเซิร์ฟเวอร์ MCP แต่ละเครื่องก่อนที่จะเพิ่มลงในพอร์ทัล
- **การตรวจสอบสิทธิ์:** ตรวจสอบสิทธิ์การเข้าถึงพอร์ทัลของผู้ใช้ตามข้อมูลประจำตัว การเข้าถึงเซิร์ฟเวอร์ MCP ในระดับขอบเขตจะขึ้นอยู่กับสิทธิ์ที่น้อยที่สุด
- **การเชื่อมต่อ:** เชื่อมต่อเซิร์ฟเวอร์ MCP ที่สามารถเข้าถึงได้ทั้งหมดด้วย URL เดียว แทนที่จะกำหนดค่าเซิร์ฟเวอร์ MCP แต่ละเครื่องแยกกัน
- **การจัดการแบบรวม:** บังคับใช้นโยบายการเข้าถึงแบบละเอียดในระดับเดียวกันสำหรับการเชื่อมต่อ AI แบบเดียวกับที่คุณทำกับผู้ใช้ที่เป็นมนุษย์
- **ปรับแต่งเครื่องมือสำหรับแต่ละพอร์ทัล:** เลือกเครื่องมือเฉพาะและเทมเพลต prompt ที่มีให้สำหรับผู้ใช้แต่ละคน

หมายเหตุ: พอร์ทัลเซิร์ฟเวอร์ MCP ของ Cloudflare รองรับเซิร์ฟเวอร์ MCP ใด ๆ รวมถึง (แต่ไม่จำกัดเพียง) เซิร์ฟเวอร์ MCP ระยะไกลใด ๆ ที่สร้างหรือปรับใช้ บน Cloudflare ความสามารถนี้พร้อมใช้งานเป็นการควบคุม การเข้าถึงเครือข่าย Zero Trust (ZTNA)

เรียนรู้เพิ่มเติมเกี่ยวกับวิสัยทัศน์ของเราได้จากบล็อกนี้

พร้อมสำรวจวิธีที่ Cloudflare นำมาใช้เพื่อช่วยรักษาความปลอดภัยขณะที่คุณใช้งาน AI แล้วหรือยัง

ขอเข้าร่วมเวิร์คช็อป

 02 026 0652 | enterprise@cloudflare.com | www.cloudflare.com REV:BDES-8382-OCT2025