جوجل تشترط استخدام MCP أو CLI لوكلاء الذكاء الاصطناعي في Workspace اعتباراً من فبراير 2027



أعلنت جوجل هويات مستقلة للوكلاء وموافقات بشرية وفحصاً لحقن الأوامر في Workspace وGoogle Cloud. وسيُلزَم وكلاء الذكاء الاصطناعي باستخدام خوادم MCP أو CLI مع بدء الإنفاذ في 1 فبراير 2027.

- بموجب ملحق أدوات الذكاء الاصطناعي في Workspace يجب أن يتصل الوكلاء عبر خوادم MCP أو CLI، ويبدأ الإنفاذ التقني في 1 فبراير 2027.
- يمكن للتطبيقات التقليدية مواصلة استخدام واجهات REST الحالية.
- يلزم الوكلاء الخارجيين معرّفات OAuth مخصصة ونطاقات بأقل صلاحية وحصصاً، وتبدأ الفوترة المرتبطة بالحصص في 1 أبريل 2027.
- تتطلب الإجراءات الحساسة مثل إرسال البريد أو تعديل مشاركة Drive تأكيداً من المستخدم.
- يمنع الملحق التخزين الدائم للبيانات الخام واستخدامها في تدريب النماذج وجمع البيانات عبر API،

> ويحدد الاحتفاظ بالمعلومات التقنية لدى جوجل بـ30 يوماً.

أعلنت جوجل حزمة ضوابط لوكلاء الذكاء الاصطناعي المستقلين الذين يصلون إلى بيانات المؤسسات والبنية السحابية عبر Google Workspace وGoogle Cloud، كما أتاحت خوادم (Model Context Protocol (MCP وواجهة سطر الأوامر (CLI) لـ Workspace للاستخدام العام.

ما الذي يتغير

بموجب ملحق أدوات الذكاء الاصطناعي الجديد في Workspace، يجب أن يتصل وكلاء الذكاء الاصطناعي عبر خوادم MCP أو CLI، ويبدأ الإنفاذ التقني في 1 فبراير 2027. أما التطبيقات التقليدية فتواصل استخدام واجهات REST الحالية. وتغطي خوادم MCP خدمات Gmail وDrive وDocs وSheets وSlides وCalendar وChat وTasks، وتُفحص الطلبات وفق صلاحيات المؤسسة وسياسات DLP وتصنيفات البيانات.

ويجب على الوكلاء الخارجيين استخدام معرّفات OAuth مخصصة ليتمكن المسؤولون من تمييزهم عن التطبيقات العادية. وتنطبق نطاقات بأقل صلاحية وحصص استخدام، وتبدأ الفوترة المرتبطة بالحصص في 1 أبريل 2027. وفي Google Cloud يحصل كل وكيل على هوية مستقلة عبر Agent Registry، وتفحص Agent Gateway الطلبات بحثاً عن حقن الأوامر باستخدام Model Armor.

التعامل مع البيانات والرقابة

يمنع الملحق التخزين الدائم لبيانات Workspace الخام واستخدامها في تدريب النماذج وجمع البيانات عبر API دون إذن. ويُحدَّد الاحتفاظ بالمعلومات التقنية لدى جوجل، مثل المتجهات وفهارس الذاكرة، بـ30 يوماً. ويجب على مزودي الأدوات حذف بيانات المستخدم والمعلومات التقنية المرتبطة بها عند فصل التكامل أو إلغاء الصلاحية.

ويستطيع المسؤولون تدقيق نشاط الوكلاء وإلغاء الوصول من لوحة الإدارة. وتوصي جوجل بمراجعة التطبيقات والوكلاء المتصلة، وضبط سياسات DLP ومراقبة سجلات OAuth، فيما يُنصح المطورون بترحيل تكاملاتهم وإضافة تأكيد المستخدم والحماية من حقن الأوامر قبل الموعد النهائي.

ما يجب فعله الآن

1. حصر وكلاء الذكاء الاصطناعي والأدوات الخارجية المتصلة بـ Workspace وGoogle Cloud وتحديد مالك لكل منها.
2. تحديد التكاملات التي ما زالت تستخدم واجهات REST لسلوك الوكلاء والتخطيط لترحيلها إلى MCP أو CLI قبل 1 فبراير 2027.
3. مراجعة سياسات DLP وتصنيفات البيانات لضمان حوكمة طلبات الوكلاء.
4. مراقبة سجلات نشاط OAuth وإلغاء الصلاحيات غير المستخدمة أو الواسعة النطاق.
5. تقييم مزودي أدوات الذكاء الاصطناعي وفق شروط الملحق للاحتفاظ والحذف وعدم التدريب، بما يشمل التزامات نظام حماية البيانات الشخصية.
6. اشتراط تأكيد بشري للإجراءات الحساسة للوكلاء مثل المشاركة الخارجية وتغيير صلاحيات IAM.