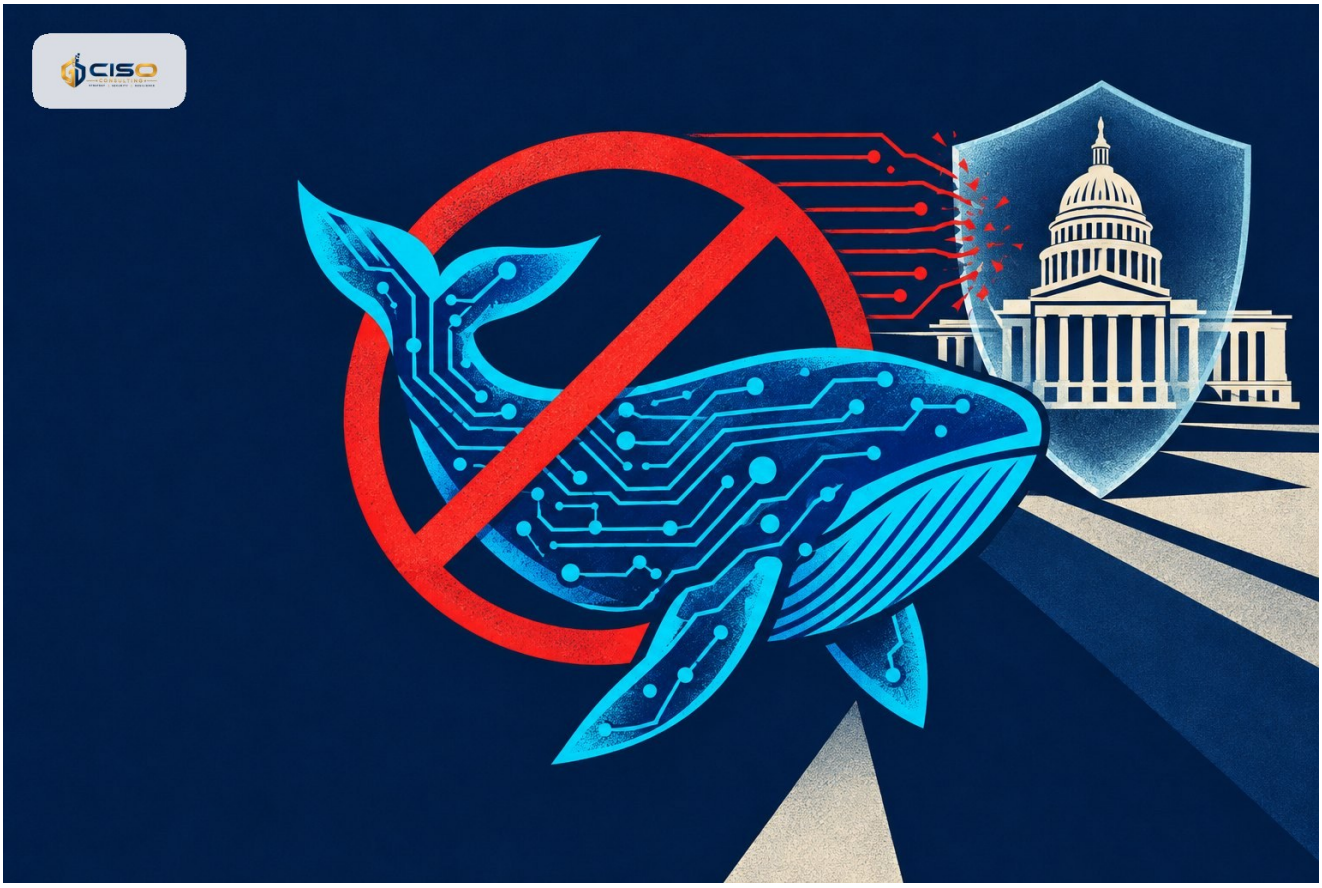
وزارة الأمن الداخلي الأمريكية تأمر الجهات المدنية الاتحادية بإزالة منتجات DeepSeek



أمرت وزارة الأمن الداخلي الأمريكية الجهات المدنية الاتحادية بالتوقف عن شراء منتجات DeepSeek واستخدامها، بما فيها منتجات الشركات التابعة والخدمات المبنية عليها، لمخاوف تتعلق بالبيانات والأمن.

- على الجهات استبعاد منتجات DeepSeek من المشتريات وإزالتها من أنظمتها، أو طلب استثناء.
- يشمل النطاق منتجات الشركات التابعة والخدمات الخارجية المبنية على تقنية DeepSeek.
- تُقدَّم طلبات الاستثناء خلال 60 يومًا، وتصدر CISA قرارها كتابيًا بالقبول أو الرفض.
- تشير الوزارة إلى مخاوف من وصول الحكومة الصينية وجمع البيانات الشخصية ونقل بيانات حكومية حساسة.
- ينطبق الأمر على الجهات المدنية الاتحادية ولا يمثل حظرًا عامًا على الاستخدام الخاص أو الفردي.

أصدرت وزارة الأمن الداخلي الأمريكية (DHS) أمرًا يُلزم الجهات المدنية الاتحادية بالتوقف عن استخدام منتجات DeepSeek وإزالتها من الأنظمة الحكومية، ونُشر الأمر في السجل الاتحادي.

ما يتطلبه الأمر

على الجهات أن تستبعد المنتجات المشمولة فورًا من المشتريات، بما في ذلك قوائم المنتجات المعتمدة ومنصات الشراء، وأن تزيلها من أنظمة تقنية المعلومات أو تطلب استثناءً. تُقدَّم طلبات الاستثناء خلال 60 يومًا من تاريخ الإصدار مع المبررات وإجراءات خفض المخاطر المقترحة، وتراجعها CISA وترد كتابيًا. وللجهات غير القادرة على الامتثال بسبب قيود في قدراتها الداخلية أن تحصل على مساعدة فنية من CISA.

لا يقتصر النطاق على روبوت المحادثة وخدمات واجهة البرمجة التابعة لـDeepSeek، بل يشمل منتجات الشركات التابعة لها والمنتجات أو الخدمات الخارجية المبنية على تقنيتها.

دوافع القرار

تشير الوزارة إلى مخاوف من وصول الحكومة الصينية إلى بنية DeepSeek التحتية، وجمع معلومات شخصية وتتبّع المستخدمين، واحتمال نقل بيانات حكومية حساسة إلى الصين. كما يثير الأمر احتمال وجود برمجيات خبيثة في النماذج، مستشهدًا بتقرير لشركة NowSecure صدر في فبراير 2025 عن تطبيق DeepSeek على iOS، وجد إرسال بيانات غير مشفرة وخوارزميات تشفير ضعيفة وتخزينًا محليًا غير آمن ومخاطر بصمة المستخدم ومشاركة بيانات مع ByteDance.

يسري الأمر على الجهات المدنية الاتحادية الخاضعة لسلطة الوزارة فقط، وليس حظرًا عامًا على الاستخدام الخاص أو الفردي، ولا يُلزم الجهات السعودية. غير أنه مرجع مفيد لكيفية تعامل جهة حكومية مع خدمات الذكاء الاصطناعي الخارجية والمنتجات المبنية عليها.

ما يجب فعله الآن

1. حصر أدوات الذكاء الاصطناعي وواجهات البرمجة والنماذج المدمجة قيد الاستخدام، بما فيها ما يعتمده الموظفون دون موافقة، وتحديد ما يعتمد منها على تقنية DeepSeek.
2. فحص منتجات الأطراف الثالثة وخدمات SaaS بحثًا عن نماذج DeepSeek الكامنة، وطلب إفصاح الموردين عن خدمات الذكاء الاصطناعي التي يعتمدون عليها.
3. إقرار سياسة لخدمات الذكاء الاصطناعي الخارجية تشمل تصنيف البيانات وأنواع البيانات المسموح بها والموافقة المسبقة قبل الاستخدام.
4. تقييم المواقع التي قد تصل فيها بيانات سرية أو شخصية إلى خدمات ذكاء اصطناعي خارج المملكة، ومراجعتها وفق متطلبات نقل البيانات خارج المملكة في نظام حماية البيانات الشخصية.
5. إدراج تقييم خدمات الذكاء الاصطناعي ضمن مراجعات مخاطر الأطراف الثالثة وضوابط الشراء، بما يتوافق مع متطلبات الأطراف الثالثة في ضوابط الأمن السيبراني الأساسية (NCA ECC).