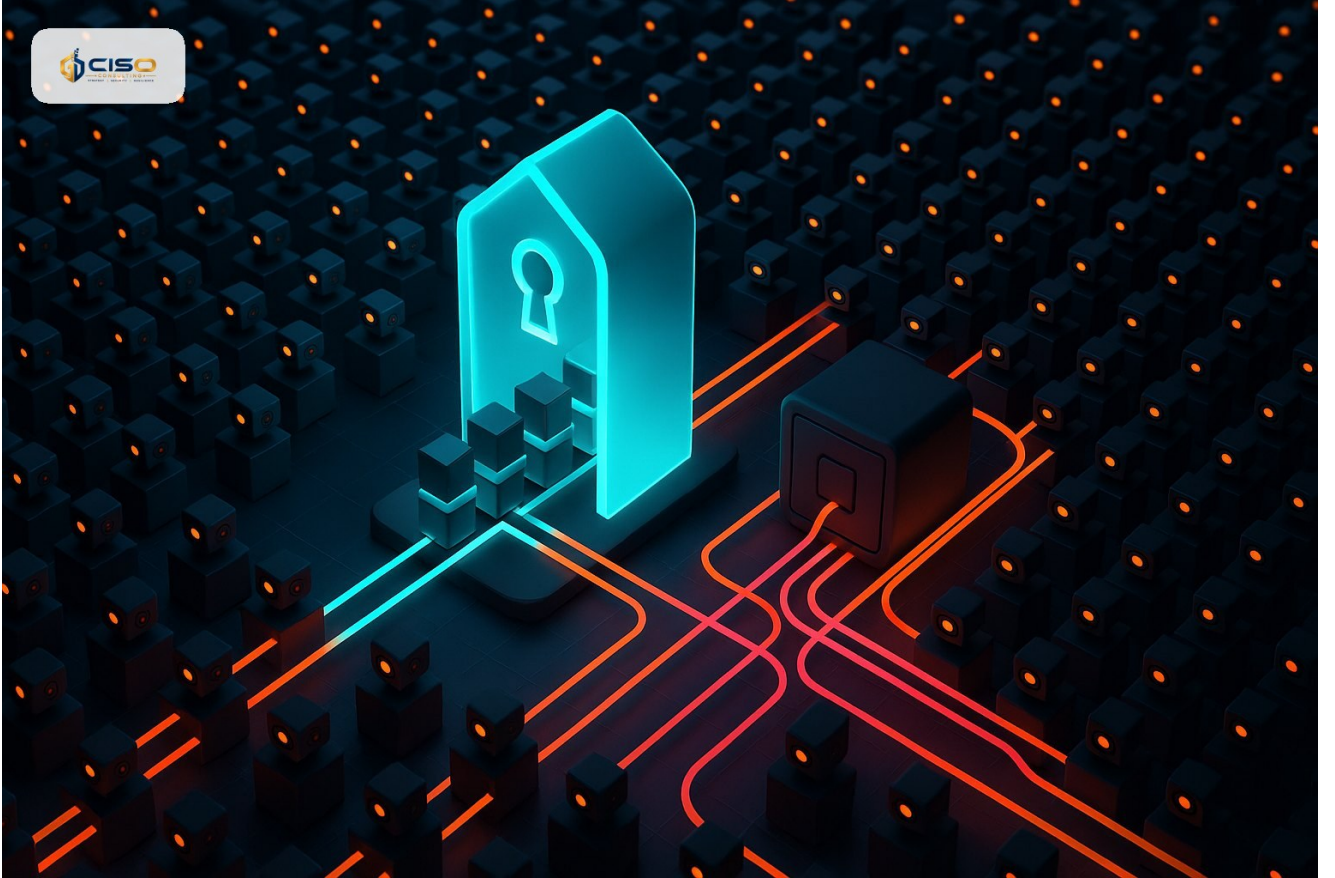


وكلاء الذكاء الاصطناعي من جهات خارجية تتجاوز ضوابط الهوية في معظم البيئات المؤسسية



تظهر الأبحاث أن حوالي 1,280 منتجاً من جهات خارجية تتضمن وكلاء ذكاء اصطناعي، منها 282 فقط خلف نظام الدخول الموحد، مما يترك نحو 1,000 غير مرئية لبنية الهوية.

- حوالي 1,280 منتجاً من جهات خارجية تتضمن وكلاء ذكاء اصطناعي في البيئات المدروسة
- 282 فقط من هذه المنتجات المدعومة بالذكاء الاصطناعي تصادق عبر أنظمة الدخول الموحد
- نحو 1,000 وكيل ذكاء اصطناعي يبقى غير مرئي لبنية الهوية بشكل افتراضي
- أنظمة الهوية لا يمكنها إلا حوكمة ما يصادق من خلالها، مما يخلق فجوة في الحوكمة
- عدم الرؤية ناتج عن التصميم وليس الإخفاء المتعمد

حجم وكلاء الذكاء الاصطناعي غير المرئية

تكشف نتائج تقرير حالة أمن الوكلاء 2026 عن تحدٍ كبير في الحوكمة للمؤسسات الخاضعة للتنظيم. في البيئات المدروسة، يتضمن حوالي 1,280 منتجاً من جهات خارجية وكلاء ذكاء اصطناعي. من بين هذه المنتجات، 282 فقط تصادق عبر أنظمة **الدخول الموحد**، مما يترك نحو 1,000 وكيل ذكاء اصطناعي يعمل خارج نطاق رؤية بنية الهوية.

هذه الفجوة لا تنتج عن إخفاء متعمد، بل تعكس قيوداً أساسياً: أنظمة الهوية لا يمكنها إلا حوكمة ما يصادق من خلالها، ومعظم وكلاء الذكاء الاصطناعي المدمجة لا تفعل ذلك أبداً. تعمل هذه الوكلاء ضمن منتجات جهات خارجية قد تمتلك بالفعل وصولاً إلى الأنظمة المؤسسية، لكن مكونات الذكاء الاصطناعي نفسها تبقى غير مسجلة لدى ضوابط الهوية المركزية.

التداعيات على المؤسسات السعودية

بالنسبة للمؤسسات الخاضعة لأطر الهيئة الوطنية للأمن السيبراني ومؤسسة النقد العربي السعودي، يمثل هذا فجوة في الضوابط. **وكلاء الذكاء الاصطناعي من جهات خارجية** التي تتجاوز بنية الهوية لا يمكن جردها أو مراقبتها لرصد تصعيد الصلاحيات أو تدقيقها عبر أدوات إدارة الهوية والوصول التقليدية. قد تعالج هذه الوكلاء بيانات حساسة أو تتخذ قرارات أو تتفاعل مع أنظمة أخرى دون الظهور في سجلات الوصول أو لوحات الحوكمة.

التحدي معماري بطبيعته. الضوابط الأمنية المصممة للأنظمة الذكاء الاصطناعي التي تنشرها المؤسسة صراحة لا تمتد إلى الوكلاء المدمجة في البرمجيات المستخدمة بالفعل. مع تحول قدرات الذكاء الاصطناعي إلى ميزات قياسية في برمجيات المؤسسات، سيزيد عدد الوكلاء غير المحكومة ما لم تكيّف المؤسسات أطر الهوية والوصول لديها للكشف عن الوكلاء التي لا تصادق بالطرق التقليدية وإدارتها.

ما يجب فعله الآن

1. إجراء جرد لجميع البرمجيات من جهات خارجية ومنصات SaaS المستخدمة حالياً لتحديد المنتجات التي قد تتضمن وكلاء ذكاء اصطناعي
2. طلب وثائق من الموردين حول قدرات الذكاء الاصطناعي ضمن برمجيات المؤسسة الحالية، بما في ذلك طرق المصادقة وأنماط الوصول للبيانات
3. تقييم ما إذا كانت أدوات إدارة الهوية والوصول الحالية قادرة على كشف أو تسجيل نشاط وكلاء الذكاء الاصطناعي المدمجة التي لا تصادق عبر الدخول الموحد
4. مراجعة العقود واتفاقيات الخدمة مع موردي الجهات الخارجية لتوضيح حقوق الحوكمة على مكونات الذكاء الاصطناعي المدمجة
5. إنشاء فريق عمل متعدد الوظائف يضم فرق إدارة الهوية والوصول والمشتريات والمخاطر لتطوير ضوابط الكشف والحوكمة لوكلاء الذكاء الاصطناعي غير المصادقة
6. تحديث استبيانات تقييم مخاطر الموردين لتشمل أسئلة محددة حول وكلاء الذكاء الاصطناعي المدمجة وتكاملها مع بنية الهوية المؤسسية