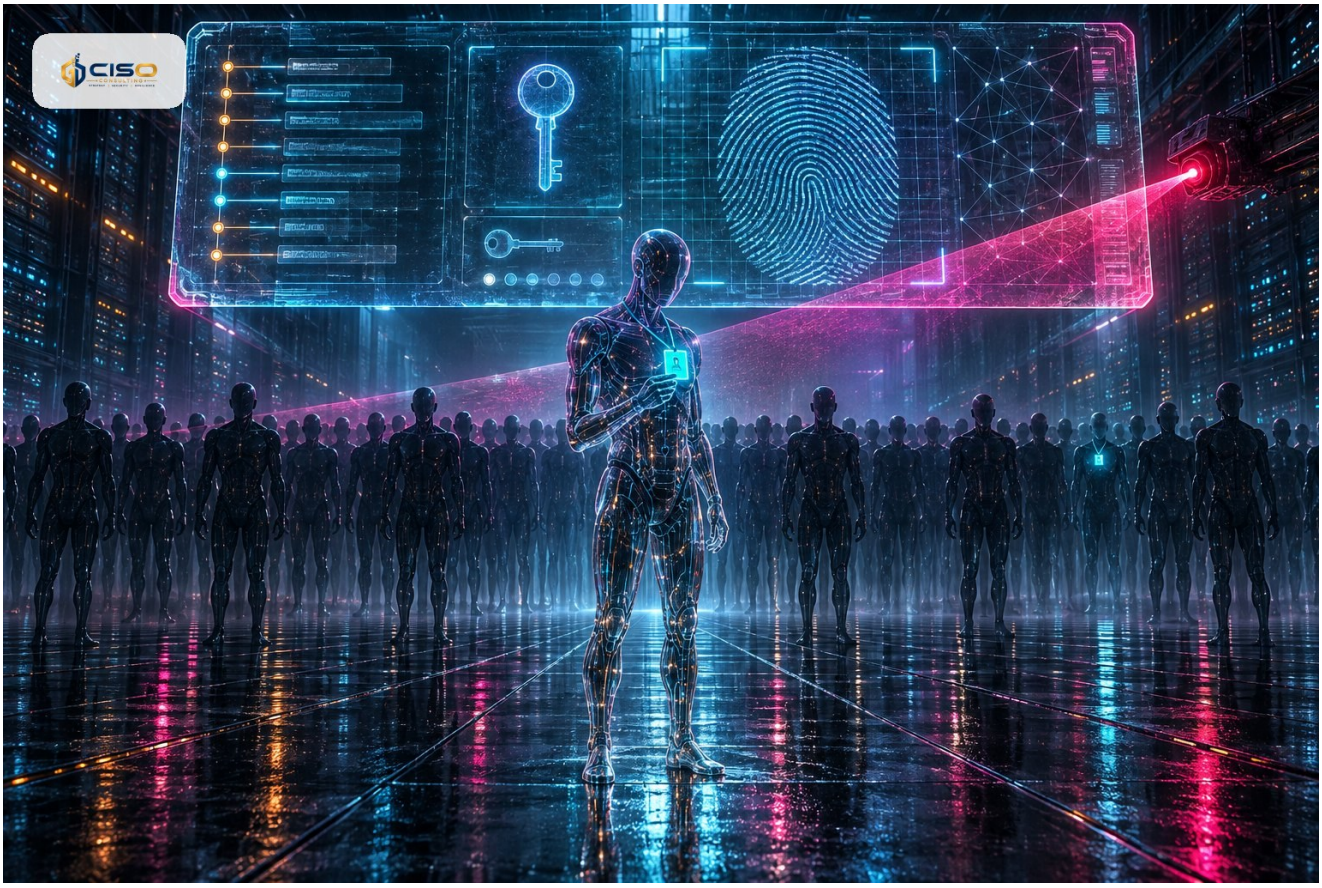
مساءلة وكلاء الذكاء الاصطناعي: توقعات SailPoint بتشديد حوكمة الهوية في 2027



تتوقع SailPoint أن يطالب المجلس والجهات التنظيمية والمؤمّنون بأدلة على حوكمة وكلاء الذكاء الاصطناعي المستقلين. وتفيد أبحاثها بأن 79% من المنشآت تشغّل وكلاء، و2% فقط طبّقت ضوابط هوية مخصصة لهم.

- تفيد SailPoint بأن 79% من المنشآت تشغّل وكلاء ذكاء اصطناعي في بيئات الإنتاج، بينما طبّقت 2% فقط ضوابط هوية مصممة لهم.
- تتوقع حادثة تعطل كبيرة في سلسلة الإمداد بسبب وكلاء أُسيئ ضبطهم ويملكون صلاحيات مفرطة.
- من الاستجابات المتوقعة: فصل المهام لأنظمة الذكاء الاصطناعي، والوصول في الوقت المناسب، والتحقق من الغرض قبل كل استدعاء API.
- يُتوقع أن يتجه المهاجمون إلى مفاتيح API ورموز OAuth وأسرار الأجهزة مع انتشار مفاتيح

المرور.

- قد تؤثر قوائم الهويات البشرية والآلية والتشفيرية في أهلية التأمين السيبراني وفي رقابة مجالس الإدارة.

تذهب توقعات SailPoint لأمن الهوية لعام 2027 إلى أن المنشآت ستُطالب ببيان الجهة المسؤولة عن أفعال وكلاء الذكاء الاصطناعي المستقلين، وأن الضغط سيأتي من الجهات التنظيمية ومجالس الإدارة والمؤمّنين. وهذه توقعات صادرة عن مزوّد وليست وقائع مؤكدة، لكنها تشير إلى فجوات عملية تستحق المراجعة الآن.

فجوة الحوكمة

تذكر أبحاث الشركة أن 79% من المنشآت نشرت وكلاء ذكاء اصطناعي في بيئات الإنتاج، بينما لدى 2% فقط ضوابط هوية مصممة لهم. كما تذكر أن 67% أمّنت وصول البشر، و24% تحكم أمن الوكلاء، وأن الهويات الآلية تفوق البشرية بنسبة 45 إلى واحد.

وتتوقع الشركة أن يتسبب وكلاء أُسيئ ضبطهم ويملكون صلاحيات مفرطة في تعطل كبير بسلسلة الإمداد، كحذف بيانات المخزون أو إنهاء عقود الموردين أو تحويل مسار الشحنات. وترى أن ذلك سيدفع نحو اشتراطات فصل المهام، بحيث لا يستطيع الوكيل تعديل صلاحياته أو تعطيل المراقبة.

الصلاحيات وبيانات الاعتماد

تتوقع SailPoint أن تتحقق بنى انعدام الثقة من هوية الوكيل ومالكه البشري وغرضه التجاري قبل كل استدعاء API، وأن يحل الوصول في الوقت المناسب محل الصلاحيات الدائمة. وتتوقع أيضًا أن تقيّد المنشآت الكبرى وصول الوكلاء الخارجيين إلى واجهاتها ما لم يثبت الشركاء هوية الوكلاء وملكيتهم ونطاق صلاحياتهم. ومع ارتفاع مفاتيح المرور إلى أكثر من 45% من عمليات دخول البشر، يُتوقع أن يركز المهاجمون على مفاتيح API ورموز OAuth وأسرار الأجهزة.

الدلالة العملية

تتوقع الشركة أن تؤثر قوائم الهويات في التقييمات والتصنيف الائتماني وأهلية التأمين السيبراني، وأن يشترط الرؤساء التنفيذيون للمعلومات والماليون ضوابط موثقة قبل تمويل مشاريع الوكلاء. وعمليًا، ينبغي للمنشآت المنظمة التعامل مع الوكلاء كهويات خاضعة للمساءلة ولها مالكون محددون.

ما يجب فعله الآن

1. حصر جميع وكلاء الذكاء الاصطناعي المستخدمين، بما فيها غير المعتمدة التي تعمل ببيانات اعتماد الموظفين، وتعيين مالك بشري معلن لكل وكيل.
2. مراجعة صلاحيات الوكلاء وفق مبدأ أقل الصلاحيات، وإزالة قدرتهم على تعديل صلاحياتهم أو تعطيل المراقبة.
3. الانتقال إلى الوصول في الوقت المناسب بدلاً من الصلاحيات الإدارية الدائمة.
4. حصر مفاتيح API ورموز OAuth وأسرار الأجهزة وتدويرها ومراقبة استخدامها.

5. اشتراط أن يوثق الأطراف الثالثة الذين يربطون وكلاءً بأنظمتكم هوية الوكيل وملكيته ونطاق وصوله.
6. إطلاع مجلس الإدارة ولجنة المخاطر على مساءلة الوكلاء وتوثيق الضوابط المطلوبة قبل تمويل أي نشر جديد.