من الرصد إلى التمكين

لماذا تعتبر الثقة والشفافية الحكم الفاصل في مستقبلك السيبراني

Proven.
Transparent.
Independent.

kaspersky

Kaspersky: ريادة واضحة في تقييمات الثقة المستقلة

جوانب التميز الأساسية

- مراكز شفافية متعددة، وقدرات مراجعة لقائمة مكونات البرمجيات (SBOM) وفحص التحديثات
- مناطق متعددة لتخزين البيانات
- تحكم تفصيلي في التحديثات وخيارات نشر مرنة
- حرية الاختيار بين خدمات السحابية أو القائمة على النشر داخل المؤسسة أو تعطيلها
- الامتناع عن الجمع غير اللازم لبيانات

الشفافية هي ميزة تفاضلية تنافسية تؤسس لثقة مستدامة بين المورّدين والعملاء والجهات التنظيمية

60 معياراً

تم تقييمها عبر محاور اختيار المستخدم، والتعامل مع البيانات، والشفافية

Proven.
Transparent.
Independent.

kaspersky

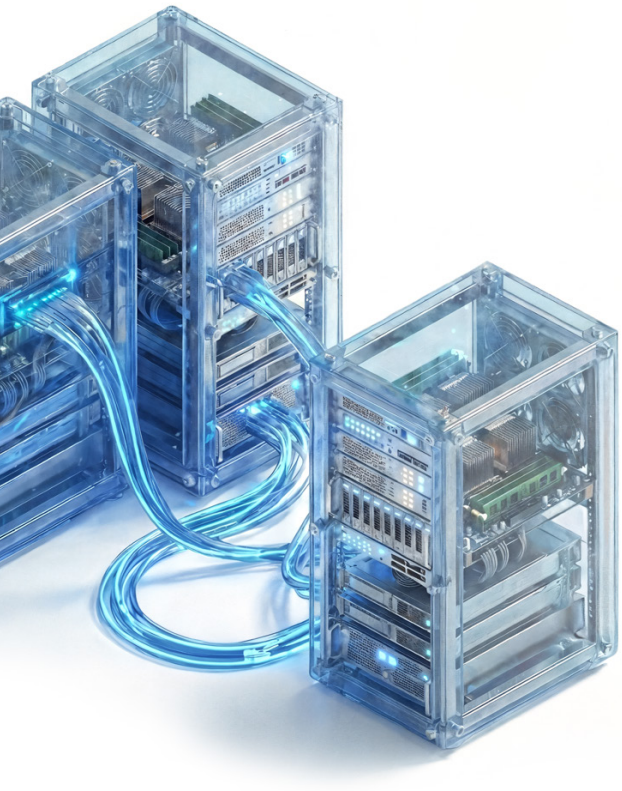
معادلة الثقة: تساؤلات جوهرية يجب على المورّد الإجابة عنه

تدفع الكُلفة المتزايدة للمخاطر السيبرانية والاشتراطات التنظيمية الحازمة وتصاعد هجمات سلاسل الإمداد، قادة الأمن إلى إعادة تقييم معمّقة بمثابة قاعدة EDR/EPP للمنظومات الحامية لكياناتهم. وبينما تعدّ منتجات صلبة للدفاعات السيبرانية، فإن صلاحيات الوصول العميق التي تتمتع بها إلى الأنظمة وقدراتها الشاملة على معالجة البيانات تستدعي طرح استفسارات حاسمة بخصوص الشفافية واستيفاء المتطلبات وبناء الثقة

تتألف النقاط المحورية للاعتبارات من الآتي

ما البيانات التي تجمعها الحلول الأمنية؟
وأين وكيف يمكن الحفاظ على هذه البيانات؟
وما مستوى التحكم المتاح للعملاء على آلية عمل هذا الحل؟
وما الأدوات التي يقدمها المورّد للتحقق من جدارة المنتج وموثوقية الشركة المصنعة؟

المورّدون الذين يوفقون بين الحلول الأمنية القوية والشفافية يضمنون المرونة التشغيلية واستيفاء المتطلبات وبناء الثقة



تقدّم (WKO) هناك دراسة مستقلة[1] كلفت بها غرفة تجارة تيرول إجابات وافية عن هذه الأسئلة المحورية

النقاط البارزة للدراسة

بينما تستوفي جميع الشركات المورّدة متطلبات الشفافية والامتثال كحد أدنى، فإن ممارساتها التشغيلية تتباين بشدة في مستوى الدقة والوضوح. وتقدم الشركات التي توفق بين الحلول الأمنية القوية والشفافية المهيكلة أعلى مستوى من اليقين بخصوص المرونة التشغيلية واستيفاء المتطلبات وبناء الثقة

الآثار المترتبة على المؤسسات

انتقاء الموردين: يجب تقييم الشفافية والاستيفاء التنظيمي كمعايير جوهرية إلى جانب قدرات الحماية
العناية الواجبة: يجب طلب الشهادات وقوائم مكونات البرمجيات وسياسات استبقاء البيانات بدلًا من الاكتفاء بالادعاءات (SBOMs) العريضة
التأهب القانوني المرتبط بالحوادث: يجب إجراء مراجعة متأنية لبنود الاستجابة للحوادث وبنود اتفاقية الملاذ الآمن وشروط الاختصاص القضائي
الخصوصية وضبط الإعدادات: يتطلب الأمر تهيئة دقيقة لخصائص القياس عن بُعد وتحميل الملفات وخدمات السُمعة من أجل تحقيق التوازن الأمثل بين المتطلبات الأمنية ومقتضيات الخصوصية

[1] "Transparency Review and Accountability in Cybersecurity," 2025 edition, commissioned by WKO (Tyrol Chamber of Commerce) and conducted by AV-Comparatives, MCI | The Entrepreneurial School®, and Studio Legale Tremolada.

Proven.
Transparent.
Independent.

kaspersky

Kaspersky وريادتها الجلية

الخصائص الفريدة التي تبلور مفهوم الثقة:

- من بين المورّدين القلائل الذين يقدمون مراكز الشفافية لعملاء الشركات الكبرى
- يوفر إمكانية الحصول على قائمة مكونات البرمجيات (SBOM) وقدرات فحص تحديث قواعد البيانات
- تتوفر لديه مرافق البيانات عبر جميع المناطق التي شملها التحليل
- تحكم كامل في نشر خدمة السُمعة سواء كانت سحابية أو قائمة على النشر داخل المؤسسة

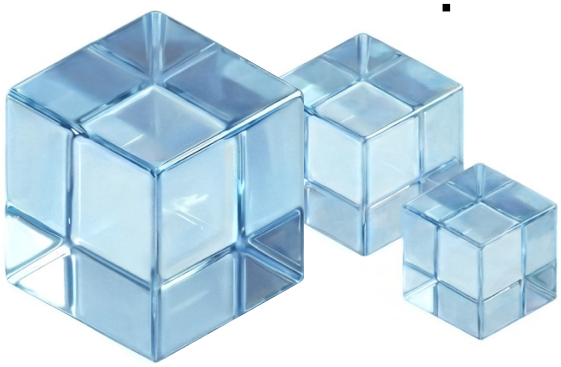
تجاوز مؤشرات الأداء المطبقة في المجال:

• أبدت Kaspersky تفوقًا في العدد الأكبر من معايير التقييم، حيث حققت أو تجاوزت المعايير المعمول بها في المجال في 75 فئة من أصل 06 فئة [2]

• تجاوزت المتوسط المطبق في المجال في كل فئة ثالثة ضمن محاور اختيار المستخدم، والشفافية، والتحكم في التحديثات، والتطوير الآمن، والاستجابة للحوادث، والتعامل مع البيانات، وتقليل حجم البيانات

أجرت الدراسة مقارنة بين مقاييس الشفافية والمساءلة التي يتبعها المورّدون الرواد في مجال الأمن السيبراني، كما قيمت ممارساتهم التجارية، والتزامهم بالمعايير القانونية الدولية، وتدابير حماية البيانات. وقد استند التحليل القانوني إلى أساس تقني لدراسة كيفية تجسيد المبادئ المُصرح بها في المنتجات. أما منتج Kaspersky الذي تم فحصه ضمن نطاق هذا البحث، فهو Kaspersky NEXT EDR Optimum.

Kaspersky تتجاوز المعايير المعمول بها في المجال في ثلث الفئات



[2] يُمكن الرجوع إلى الوثيقة المرفقة للحصول على العدّ التفصيلي للفئات والمصطلحات المحددة لها.

Proven.
Transparent.
Independent.

kaspersky

الضرورة الحتمية لتوفير الشفافية في عالم الأعمال

في حين أن استبانات التوريد تتميز بالشمولية، فإن إدراج معايير الشفافية والثقة يعالج المخاطر الجوهرية للعمليات التجارية. وتُظهر دراسة «مراجعة الشفافية والمساءلة في الأمن السيبراني» تباينًا هائلًا في مستوى صراحة الموردين — من أولئك الذين يتيحون زيارات لمراكز الشفافية وإفصاحات أمنية معمقة، إلى آخرين يعتمدون على صياغات تعاقدية عامة ومجرد ادعاءات امتثال غير محددة.[3]

ولا يقتصر هذا التفاوت على كونه تفضيلًا في عملية التوريد فحسب؛ بل يؤثر مباشرةً على المخاطر التجارية. وعند وقوع حوادث الأمن السيبراني، تصبح قدرة المؤسسة على الاستجابة بكفاءة، وإثبات العناية التنظيمية الواجبة، وصيانة ثقة أصحاب المصلحة، رهناً بمدى الفهم المسبق لممارسات المورّد. وتترجم حالة إبهام المورّد بشكل مباشر إلى ثغرات في الالتزام، وتعريض للمخاطر القانونية، ونقاط قصور تشغيلية قد تُعيق الاستجابة للحوادث.

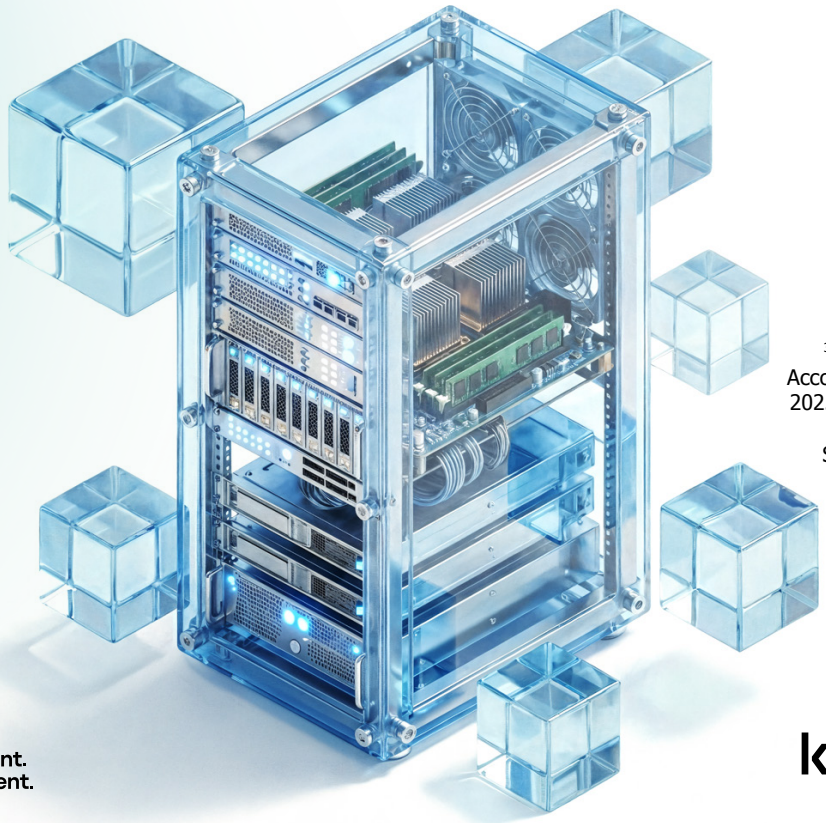
تستوجب بيئات الأعمال الحديثة درجة أكبر من المساءلة، ولا يجوز إعفاء موردي الأمن السيبراني من هذا المطلب. وتوضح الدراسة أن هناك ارتباطًا وثيقاً بين الشفافية والنضج التشغيلي — إذ يُبرهن الموردون الذين يقومون بنشر نتائج المراجعات، ويحافظون على قوائم محدّثة لمكونات البرمجيات، ويوفرون أدوات تحكم تفصيلية في الخصوصية، على ممارسات أمنية أرقى باستمرار.

أما قادة الأعمال، يجب أن يُصرّون على بناء علاقات مع المورّدين تدعم التحقق المستقل والتوثيق المفصّل وهياكل المساءلة الواضحة. ويقوم هذا المنهج بتقوية المرونة السيبرانية، ويضمن الاستيفاء للمتطلبات التنظيمية الصارمة، ويوفر ميزة تنافسية ضمن مشهد تهديدات يزداد تعقيداً.

تُسهم استنتاجات البحث مباشرةً في الارتقاء بمستوى الحوكمة، وتوجيه عمليات التوريد بناءً على معلومات دقيقة، وضمان الإدارة المسؤولة للمخاطر الرقمية

14 مورداً

رائدًا لأمن نقاط النهاية خضعوا للاختبار



[3] "Transparency Review and Accountability in Cybersecurity," 2025 edition, AV-Comparatives, MCI | The Entrepreneurial School®, and Studio Legale Tremolada, p. 39.

Proven.
Transparent.
Independent.

kaspersky

نظرة عامة على مؤشرات الأداء المطبقة في المجال

بينما غدت العديد من الممارسات، مثل التقيد بدورة حياة تطوير النظم (SDLC) معايير قياسية في القطاع، فإن والامتثال للائحة الأوروبية لحماية البيانات (GDPR)، بعضها يظل نادرًا بين الموردّين الأمنيين الـ 14 البارزين الذين خضعوا للتقييم:

المعيار	معدل الانتشار في المجال (عدد الموردّين الذين يوفرون هذه الميزة)	Kaspersky
مراكز الشفافية لمراجعة الشفرة المصدرية والتحقق من ممارسات معالجة البيانات	منخفض (14/3)	✓ نعم
إمكانية التنزيل المباشر للتوقيعات/التعريفات لغرض الفحص	متوسط (14/6)	✓ نعم
توفير قائمة مكونات البرمجيات (MOBS)	منخفض (14/3)	✓ نعم
إصدار تقارير الشفافية المنتظمة	منخفض (14/4)	✓ نعم
خدمة السُمعة القائمة على النشر داخل المؤسسة	متوسط (14/8)	✓ نعم
توفر خيارات متعددة لمراكز البيانات	منخفض (14/4)	✓ نعم
نشر الإشعارات الأمنية بصورة دورية	متوسط (14/7)	✓ نعم
إتاحة نتائج تدقيق الأمان المستقل	متوسط (14/7)	✓ نعم
توفر خيارات الطرح التدريجي للتحديثات	متوسط (14/8)	✓ نعم
إتاحة سجل تحديثات المنتجات للعامة	مرتفع (14/13)	✓ نعم
توفير التقارير العلنية حول طلبات جهات إنفاذ القانون للبيانات	متوسط (14/9)	✓ نعم
إعداد تقارير مفصلة للغاية عن الحوادث	متوسط (14/7)	✓ نعم
توفر ولايات قضائية متعددة لفض النزاعات	متوسط (14/1)	لا[4]
الالتزام بقانون حماية خصوصية المستهلك في كاليفورنيا (APCC)	مرتفع (14/12)	✓ نعم
الالتزام بقانون المرونة السيبرانية (ARC)	لا أحد (0)	لا

4 يمكن تغيير الولاية القضائية لفض النزاعات بموجب عقد منفصل (للاطلاع على المزيد، انظر الصفحة 7).

Proven. Transparent. Independent.

kaspersky

تحليل معمّق: الممارسات الجوهرية

الشفرة المصدرية وقائمة مكونات البرمجيات

يعتمد جميع المورّدين الذين تم اختبارهم على نماذج الشفرة المصدرية المغلقة، في حين أفصح 13 موردًا من أصل 14 عن استخدامهم لمكونات مفتوحة المصدر من طرف ثالث. إلا أن 3 موردين فقط هم من يديرون مراكز **شفافية** تسمح للعملاء من الشركات الكبرى بمراجعة الشفرة المصدرية.
من بين هؤلاء، يخصص أحد المورّدين إمكانية الوصول للعملاء الحكوميين فقط، بينما يحدّ آخر نطاق الوصول بالشيفرة المصدرية والملكية الفكرية غير المحددة. وتنفرد Kaspersky بتقديم أوسع عروض مراكز الشفافية، والتي تتضمن فحص قواعد اكتشاف التهديدات وإجراء تحقق للتأكد من تطابق البنيات البرمجية مع الإصدارات العامة.
ثلاثة موردين فقط، من ضمنهم Kaspersky، يوفرون للعملاء إمكانية الوصول إلى قوائم مكونات البرمجيات.

التحكم الدقيق في التحديثات

يركز العديد من المورّدين على أفضل ممارسات التحديث لديهم، مثل التنفيذ متعدد المراحل والاختبار المُحكم، وضمان الجودة. ولكن 5 موردين فقط، من ضمنهم Kaspersky، يقدمون جميع هذه الخيارات لعملائهم:

الميزة	معدل الانتشار لدى المورّد
سجل التحديثات المتاح للعامة	14/13
تنزيل تحديثات التعريفات	14/6
التحديثات التلقائية	14/14
خيارات اختبار ما قبل الإصدار	14/14
الطرح التدريجي للتحديثات	14/8

نظرة متعمقة على مركز الشفافية

تُدير Kaspersky أكثر من 10 مرافق عالمية للشفافية حيث يمكن للجهات التنظيمية الحكومية والعملاء من الشركات الكبرى القيام بمراجعة مستقلة للشفرة المصدرية، وقواعد اكتشاف التهديدات، وتحديثات البرامج، وعمليات التطوير. وتتوفر ثلاثة مستويات للتقييم: «Blue Piste» للمعاينة العامة، و «Red Piste» لتحليل الشفرة المستهدفة، و «Black Piste» للمراجعات الشاملة والمعمّقة. يمكن للزوار فحص وثائق التطوير الآمن، وإعادة بناء الشيفرة المصدرية للتحقق من تطابق الوحدات المتاحة علنًا مع البنيات البرمجية، ومراجعة تحديثات قاعدة بيانات مكافحة الفيروسات بمساعدة الخبراء.

Proven.
Transparent.
Independent.

kaspersky

الوضع الأمني

إن الإدارة القوية للثغرات الأمنية والإفصاح الشفاف وعمليات التدقيق المستقلة وعمليات دورة حياة التطوير الآمن تشكل مؤشرات على جدارة المورد بالثقة ومرونته. **إن Kaspersky وموردين آخرين هم فقط من يوفرون جميع الإمكانيات التي تم تقييمها:**

الميزة	معدل الانتشار لدى المورّد
الإبلاغ عن الثغرات الأمنية	14/14
النشرات الإرشادية الأمنية	14/7
التعاون وبنود اتفاقيات الملاذ الآمن	14/7
نتائج التدقيق الأمني	14/7
ممارسات دورة حياة التطوير الآمن	14/14

كشفت الأبحاث أنه بالإضافة إلى الأطر التنظيمية المؤكدة على نطاق واسع، يبدو أن العديد من الموردين يستعدون للتنفيذ الكامل لقانون المرونة السيبرانية (CRA). وبعد أن شاركت Kaspersky بمدخلاتها في صياغة القانون أثناء الدعوة المفتوحة لعملية التشريع، فإنها تراقب عن كثب التنفيذ المرحلي لقانون المرونة السيبرانية لتكون جاهزة لاستيفاء الالتزامات التنظيمية بمجرد دخوله حيز التطبيق الكامل.

الشفافية والسياسات

يُبيّن الإفصاح العام عن الحوادث وطلبات إنفاذ القانون مدى شفافية المورّد. وفي حين يلتزم معظم الموردين تعاقديًا بالإفصاح عن الحوادث، فإن 7 موردين فقط يوثقون الإفصاحات المفصّلة. وهناك 3 موردين فقط، بمن فيهم Kaspersky، ينشرون تقارير شفافية تتضمن تفاصيل طلبات إنفاذ القانون:

الميزة	معدل الانتشار لدى المورّد
التزام تعاقدي بالإفصاح عن الحوادث والاستجابة لها	14/13
توثيق إفصاحات الحوادث التفصيلية وفي الوقت المناسب	14/7
الإفصاح عن طلبات إنفاذ القانون للعملاء المتضررين	14/9
إصدار تقارير الشفافية	ينشرون للعامة، ومورّد واحد ينشر عند الطلب 14/3

الاستيفاء التنظيمي والشهادات

يعدّ الاستيفاء للمعايير الدولية والأطر التنظيمية والحوكمة القانونية أمرًا بالغ الأهمية لشفافية المورّد وثقته. وقد وجدت الدراسة أن جميع الموردين يؤكدون استيفاءهم للائحة العامة لحماية البيانات (GDPR) ويحتفظون بشهادات ISO/IEC 10072 و SOC 2 Type II. **يلتزم 12 موردًا من أصل 14، بما فيهم Kaspersky، بقانون حماية خصوصية المستهلك في كاليفورنيا.** ويوفر أحد عشر موردًا خيارات متعددة لولايات قضائية لفض النزاعات. وفي حين يغيب هذا النص عن الاتفاقية العامة لدى Kaspersky، إلا أنها تتضمن شروطًا تخول العملاء استبدال الاتفاقية العامة بترتيبات تعاقدية فردية تلبي هذا المطلب.

kaspersky

Proven.
Transparent.
Independent.

4 موزّدين

لديهم مرافق بيانات عبر جميع المناطق التي شملها التحليل

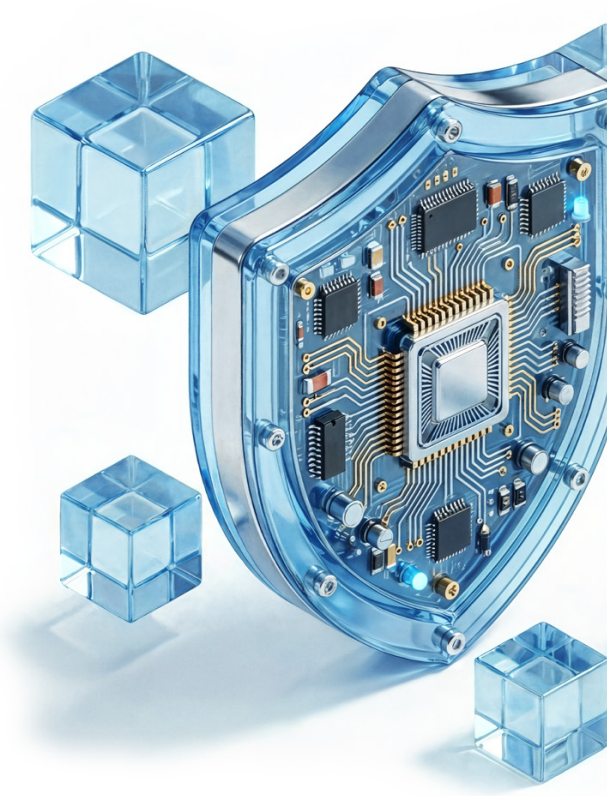
القياس عن بُعد وتخزين البيانات

إن أسلوب إدارة الموزّدين لبيئات نشر المنتجات وجمع بيانات القياس عن بعد وتخزين البيانات يُعد أمرًا بالغ الأهمية لكل من الشفافية والاستيفاء للمتطلبات. وتعمل خيارات النشر المرنة والمعالجة الشفافة للبيانات على تقوية جدارة المورّد بالثقة. ورغم شيوع التشغيل في وضع عدم الاتصال، فإن نصف الموردين فقط يوفرون بدائل لخدمة السُمعة السحابية، **وأربعة فقط يحافظون على مرافق بيانات** عبر جميع المناطق التي تم تحليلها — **وتوفر Kaspersky كلتا الميزتين:**

الميزة	معدل الانتشار لدى المورّد
دعم التشغيل في وضع عدم الاتصال/في بيئات معزولة	14/14
خدمة السُمعة القائمة على النشر داخل المؤسسة	14/8
إخفاء الهوية والحذف الدوري للبيانات	14/14
توافر مراكز بيانات في الاتحاد الأوروبي	14/14
توافر مراكز بيانات في أمريكا الشمالية	14/14
توافر مراكز بيانات في الشرق الأوسط	14/4

تحليل نقل البيانات

صُممت منتجات الشركات الكبرى التي تم اختبارها لجمع ونقل البيانات كجزء من عملية تشغيلها العادية، لكي تكون قادرة على توفير الحماية ضد التهديدات. وقد يمثل كل عنصر بيانات قياسًا أمنيًا مهمًا عن بُعد، ولكنه قد يُصنف أيضًا كمعلومات حساسة يتم إرسالها إلى مركز بيانات طرف ثالث.
يتعين على المنظمات مواءمة عملية جمع البيانات مع مستويات المخاطر والأولويات الخاصة بها عبر خيارات الضبط المتاحة.



أظهرت Kaspersky الحد الأدنى من جمع البيانات أثناء الاختبار

حيث لاحظ الباحثون أن المنتج ينقل المؤشرات الأكثر شيوعًا (مثل اسم المضيف، واسم مستخدم Windows، وعنوان IP الداخلي) بالتساوي مع جميع المنافسين، بينما تجنب البيانات الحساسة مثل سجلات الأعطال.
تسمح Kaspersky أيضًا بتعطيل شبكة أمن Kaspersky (التي تشمل إرسال سُمعة الملفات) وتعطيل وظيفة اكتشاف نقطة النهاية والاستجابة بشكل تام.

Proven.
Transparent.
Independent.

kaspersky

بنود العمل المقترحة لكبار مسؤولي أمن المعلومات

1. عناصر الشفرة المصدرية والمنتجات

- ☐ المطالبة بكشف تفصيلي لقائمة مواد البرمجيات (SBOM) خلال التوريد ولأغراض الإدارة المستمرة للمخاطر
- ☐ التثبت من إجراءات المورّد الخاصة برصد نقاط ضعف سلسلة التوريد والتخفيف من حدتها
- ☐ السعي لمعرفة إمكانية النفاذ إلى مراكز الشفافية لمراجعة الشفرة المصدرية والتحقق من البنيات البرمجية

2. إدارة التغييرات وتحديثات المنتجات

- ☐ اشتراط توفير الوصول إلى سجلات التغيير المفصلة ومذكرات الإصدار
- ☐ التثبت من برامج الطرح التدريجي والاختبار التجريبي لأغراض المصادقة قبل عملية النشر

3. تخزين البيانات والخصوصية والقياس عن بُعد

- ☐ المطالبة بتوفير إعدادات خصوصية واضحة وقابلة للضبط لبيانات القياس عن بُعد، وتحميل الملفات، وعمليات تجميع البيانات
- ☐ اشتراط تحديد جداول زمنية صريحة للاحتفاظ بالبيانات، وإجراءات الحذف، ومواقع مراكز البيانات
- ☐ التحقق من دعم عمليات النشر في وضع عدم الاتصال أو في البيئات المعزولة

4. الوضع الأمني والاستجابة للحوادث والسياسات

- ☐ اشتراط تقديم تقارير شفافة عن الثغرات الأمنية والنشرات الاستشارية الأمنية العامة
- ☐ طلب نتائج تدقيق الطرف الثالث ووثائق دورة حياة التطوير الآمن
- ☐ التأكد من أن الالتزامات التعاقدية تتضمن الإخطار العاجل بانتهاك البيانات وتقديم تقارير مفصلة عن السبب الجذري، والنطاق، والإجراءات التصحيحية
- ☐ مراجعة سجل المورّد في الإفصاحات العلنية للحوادث ووضوح استجابته
- ☐ السعي للحصول على تقارير الشفافية الدورية وسياسات التعامل مع طلبات جهات إنفاذ القانون

5. الاستيفاء التنظيمي والشهادات

- ☐ التحقق من نطاق الشهادة (ISO/IEC 27001, SOC 2) من خلال الوثائق الرسمية، وليس مجرد الشعارات أو المطالبات
- ☐ التأكد من أن الشهادات تغطي بشكل صريح مراكز البيانات، وأنظمة البناء، والخدمات السحابية

Proven.
Transparent.
Independent.

kaspersky

مواصلة رحلة الشفافية

قراءة التقرير الكامل

استكشاف Kaspersky
Next EDR Optimum

تحديد موعد لزيارة مركز
الشفافية

الاطلاع على تقرير
Kaspersky للشفافية

استكشاف محفظة
Kaspersky المتكاملة
لمنتجات الشركات الكبرى

Proven.
Transparent.
Independent.

kaspersky