واقع الشبكات اللاسلكية في عام 2026

قوة التأثير المضاعف: كيف تساهم الاستثمارات الاستراتيجية في الشبكات اللاسلكية بتسريع نمو المنظمات في عصر الذكاء الاصطناعي

المملكة العربية السعودية

ملخص تنفيذي

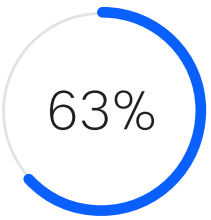
إن شبكة الواي-فاي في عام 2026 ليست مجرد أداة تكميلية، بل هي محرك استراتيجي للنمو، فعلى المستوى العالمي، أظهرت البيانات أن المنظمات التي تعتمد على الاستثمار الشامل في الشبكات اللاسلكية تزيد من احتمالية تحقيقها لعائد قوي على الاستثمار بمقدار أربعة أضعاف، مع تحقيق مكاسب ملموسة عبر جميع وظائف الأعمال، بدءاً من الكفاءة التشغيلية وصولاً إلى نمو الإيرادات. ويُعد هذا التأثير المضاعف عاملاً قوياً يميز الاستثمارات في الشبكات اللاسلكية عن غيرها من استثمارات تقنية المعلومات، إذ يساهم في تحقيق عوائد تراكمية وشاملة للشركة.

ومع ذلك، يُشير 98% من المنظمات إلى أن درجة التعقيد في الشبكات اللاسلكية تتصاعد، والتهديدات السيبرانية تتزايد، في ظل وجود نقص حاد في الكفاءات المتخصصة القادرة على التعامل مع هذه التحديات. لذلك، يتعيّن على المنظمات التكيّف مع احتياجات الاتصال المتنوعة وتمكين منظومة متكاملة من المستخدمين والأجهزة، بدءاً من الموظفين والمقاولين وصولاً إلى الروبوتات الذاتية، وأجهزة الاستشعار الذكية، والتطبيقات المدعومة بالذكاء الاصطناعي.

تتمتع المنظمات العالمية التي تتبنى الاستثمار الشامل في الذكاء الاصطناعي والأتمتة وأحدث الحلول السيبرانية إضافةً إلى الكفاءات المعتمدة بميزة تنافسية واضحة مقارنةً بتلك التي لا تعتمد هذا النهج، حيث تُحقق:

+4x

زيادة بمقدار 4 أضعاف في احتمالية تحقيق عوائد قوية على استثماراتها في مجال الشبكات اللاسلكية



ارتفاع بنسبة 63% في متوسط عائد الاستثمار على الاستثمارات في الشبكات اللاسلكية

يكشف هذا التقرير عن "مفارقة الذكاء الاصطناعي في الشبكات اللاسلكية": فالذكاء الاصطناعي هو المحرك الرئيسي لعائد الاستثمار والمصدر الأكبر للمخاطر المتصاعدة في آن واحد. وعلى الرغم من أن العمليات القائمة على الذكاء الاصطناعي توفر مئات الساعات سنوياً لكل متخصص في تقنية المعلومات، إلا أنها تزيد أيضاً من متطلبات البنية التحتية، والتهديدات السيبرانية، ونقص الكفاءات المتخصصة.
يكشف بحثنا أن البنى التحتية القديمة، إلى جانب ثلاثة تحديات مترابطة، تساهم في الحدّ من قدرة المنظمات على تحقيق عائد الاستثمار بشكل كامل من الشبكات اللاسلكية. وتشمل هذه التحديات تعقيد العمليات، وتزايد التهديدات السيبرانية، واتساع فجوة الكفاءات. كما تتفاعل هذه العوامل فيما بينها، مما يؤدي إلى تراكم المخاطر وتفاقمها على مستوى الشركة. يتمحور هذا البحث حول شبكة الواي-فاي باعتبارها الركيزة الأساسية للاتصال في المنظمات، مع تسليط الضوء على منظومة الشبكات اللاسلكية وما تتيحه من تطبيقات مدعومة بالذكاء الاصطناعي، وبيئات إنترنت الأشياء وتكنولوجيا تشغيلية، فضلاً عن حالات الاستخدام المبتكرة في المنظمات.

وتظهر النتائج أن المنظمات التي تعالج هذه التحديات التشغيلية والسيبرانية والبشرية بشكل متكامل تحقق عائداً على الاستثمار أعلى بنسبة 63% مقارنة بتلك التي لا تتبع هذا النهج، ما يؤكد أن الاستثمار الاستراتيجي في الشبكات اللاسلكية يحقق عوائد ملموسة ومتراكمة في عدة جوانب. وهذا يفسر تسارع وتيرة الاستثمار في الشبكات اللاسلكية، لا سيما مع التوسع المتزايد في استخدام الذكاء الاصطناعي وتطور الابتكار التقني.

تشير النتائج بشكل عام إلى أن منظمات المملكة العربية السعودية التي تمنح أولوية استراتيجية للشبكات اللاسلكية، ستحقق مكاسب ملموسة عبر عدة أصعدة، إذ يفيد أكثر من 83% بتحسن في تفاعل العملاء، و78% في الكفاءة التشغيلية، و75% في إنتاجية الموظفين، بينما يسجل 67% تأثيراً إيجابياً على الإيرادات. ويؤكد ذلك أن البنية التحتية المتطورة للشبكات اللاسلكية تساهم بشكل مباشر في تحقيق نمو الأعمال.
تمثل المرحلة الحالية فرصة حقيقية لتحقيق ميزة تنافسية. فالمنظمات في المملكة العربية السعودية التي تتخذ خطوات حاسمة خلال عام 2026 - عبر تبسيط العمليات، وتعزيز أمن الشبكات اللاسلكية، وبناء كوادر بخبرات معتمدة - ستكون الأقدر على تحويل شبكة الواي-فاي إلى محرك استراتيجي للنمو خلال العقد المقبل.

استراتيجية الشبكات اللاسلكية في مواجهة التحديات:
التعامل مع مفارقة الذكاء الاصطناعي والعوائق التي تحدّ من تحقيق العائد على الاستثمار

تعريف مفارقة الذكاء الاصطناعي في الشبكات اللاسلكية وأهميتها

تُشكل مفارقة الذكاء الاصطناعي في الشبكات اللاسلكية التحدي الاستراتيجي الأهم لقادة الأعمال في المملكة العربية السعودية لعام 2026 والفرصة الأثمن للمبادرين في آنٍ واحد. فبينما يبرز الذكاء الاصطناعي كمحرك أول لعوائد الاستثمار في الشبكات اللاسلكية، فإنه يظل مصدراً أساسياً لتحدياته المتنامية. وعلى المستوى العالمي، تؤكد نتائج هذا البحث أن المنظمات التي تدمج تحسين الشبكات اللاسلكية في صميم استراتيجيات الذكاء الاصطناعي لا تكتفي بتعزيز أهميتها الاستراتيجية فحسب، بل تحقق عوائد استثنائية تفوق نظيراتها، وذلك رغم ما يفرضه الذكاء الاصطناعي من تعقيدات تشغيليّة غير مسبوقة، وتهديدات أمنية متطورة، وتنافس كبير على استقطاب الكفاءات الماهرة.

مفارقة الذكاء الاصطناعي في الشبكات اللاسلكية

الذكاء الاصطناعي هو الحل والتحدي في آن واحد

التحدي

- الهجمات السيبرانية المولدة بالذكاء الاصطناعي تشكل تهديداً أمنياً كبيراً
- نقص في الكفاءات المتخصصة في مجالي الشبكات اللاسلكية المتقدمة والذكاء الاصطناعي
- استنزاف الكفاءات التقنية من مجال الشبكات اللاسلكية إلى الذكاء الاصطناعي

الحل

- العمليات المدعومة بالذكاء الاصطناعي تساهم في تبسيط تعقيدات الشبكات اللاسلكية
- الأتمتة تتيح لفرق تقنية المعلومات التركيز على الاستراتيجية
- تسريع عملية تذاكر الدعم الفني وسير العمل

الذكاء الاصطناعي هو العامل الأهم لتحقيق عائد على الاستثمار في الشبكات اللاسلكية - لكنه أيضاً أكبر مصدر للمخاطر.

التحديات المتعددة التي يفرضها الذكاء الاصطناعي على فرق الشبكات اللاسلكية

أبرز الصعوبات في توظيف الكفاءات	أبرز المجالات التي تُبعد الكفاءات عن الشبكات اللاسلكية	أبرز عوامل التهديدات السيبرانية
#1 قلة المرشحين ذوي المهارات المتقدمة في الشبكات اللاسلكية أو المهارات المدمجة مع الذكاء الاصطناعي	**#1** الذكاء الاصطناعي وتعلم الآلة	**#1** الهجمات السيبرانية المولدة أو المؤتمتة بالذكاء الاصطناعي
#2 قيود الميزانية الداخلية أو تجميد التوظيف	**#2** الأمن السيبراني	**#2** زيادة استخدام إنترنت الأشياء والأجهزة المتصلة
#3 القيود الجغرافية أو تحديات العمل عن بُعد	**#3** هندسة البرمجيات وتطوير التطبيقات	**#3** قلة الكفاءات أو القدرة التشغيلية لمراقبة التهديدات والاستجابة لها

تتباين رؤية المنظمات في المملكة العربية السعودية لأهمية الشبكات اللاسلكية بناءً على مستوى تبنيها للذكاء الاصطناعي. ووفقاً للإحصائيات العالمية في هذا البحث، يرى 56% من قادة المنظمات التي توظف الذكاء الاصطناعي أن هذه الشبكات تمثل أهمية استراتيجية قصوى، بينما تنخفض هذه النسبة إلى 46% فقط لدى المنظمات التي لم تعتمد بعد تقنيات الذكاء الاصطناعي.

تستند هذه الأهمية الاستراتيجية المتزايدة إلى حقيقة جوهرية: وهي أن تطبيقات الذكاء الاصطناعي تتطلب شبكات لاسلكية ذات أداء أعلى وقدرة أكبر على الصمود في وجه الهجمات السيبرانية. لذا، فإن المنظمات التي نجحت في مواءمة تحسين بنيتها التحتية مع خطط تطبيق الذكاء الاصطناعي قد حققت بالفعل عوائد استثنائية. ويظهر هذا بوضوح في المملكة العربية السعودية، حيث أكد أكثر من 70% من قادة الأعمال أن الاستثمار الذكي في الشبكات اللاسلكية كان العامل المباشر لقفزات ملموسة في الكفاءة التشغيلية، وتفاعل العملاء، وإنتاجية الكوادر، وصولاً إلى تعزيز الإيرادات النهائية.

كيف تترابط فرص وتحديات ومخاطر تطورات الذكاء الاصطناعي؟

بينما يُنظر إلى الذكاء الاصطناعي كوسيلة لتبسيط عمليات الشبكات اللاسلكية ومعالجة تعقيدها، تشكل الهجمات السيبرانية الناتجة عن الذكاء الاصطناعي أو الهجمات المؤتمتة أحد أبرز العوامل لارتفاع التهديدات السيبرانية في الشبكات اللاسلكية، وقد أدى هذا الواقع إلى تحوّل في خارطة المواهب، إذ بات مجال الأمن السيبراني يستقطب الكفاءات التقنية، مما تسبب في استنزاف الكوادر المتخصصة في الشبكات اللاسلكية في المملكة العربية السعودية.

العائق الأول: التعقيد التشغيلي يفوق القدرات الراهنة

يُشكل التعقيد التشغيلي المتزايد العائق الأبرز الذي يحول دون قدرة المنظمات على حل مفارقة الذكاء الاصطناعي في الشبكات اللاسلكية. فقد أفاد 100% من قادة مجال الشبكات اللاسلكية في المملكة العربية السعودية بأن عملياتهم تشهد تعقيداً مطرداً، مما دفع المنظمات إلى تبني منهجية "رد الفعل". هذا الوضع لا يستنزف الموارد ويعطل المسارات الاستراتيجية فحسب، بل يقوّض بشكل مباشر مبادرات أتمتة العمليات التي صُممت في الأصل لتقليص هذا التعقيد. وقد أدى ذلك إلى نشوء حلقة مفرغة: التعقيد يفرض وتيرة عمل قائمة على معالجة الأزمات الفورية، وهذا النوع من العمل يعيق جهود التحديث، بينما يؤدي غياب التحديث بدوره إلى ترسيخ التعقيد وإدامته.

وتُرجع المنظمات في المملكة العربية السعودية هذا التعقيد المتزايد إلى ثلاثة عوامل رئيسية: أعباء الأعمال الحيوية التي تشمل أنظمة تقنية المعلومات، وإنترنت الأشياء، والتكنولوجيا التشغيلية والاعتماد المتزايد على التطبيقات المدعومة بالذكاء الاصطناعي بنسبة (50%)، وزيادة الطلب على النطاق الترددي الناتج عن ظهور حالات استخدام مبتكرة بنسبة (36%)، والحاجة الملحة لتحجيم المخاطر السيبرانية الناشئة بنسبة (35%).

هذا التعقيد ليس مجرد تحدٍ نظري، بل يترجم إلى ضغوط تشغيلية ملموسة، حيث يفيد 40% بأن فرقهم تتلقى ما لا يقل عن 50 تذكرة دعم فني للشبكة اللاسلكية أسبوعياً، مما يعني استهلاك مئات الساعات شهرياً من وقت فرق تقنية المعلومات في إدارة ومعالجة هذه البلاغات الروتينية، بدلاً من التركيز على الابتكار.

ومن أبرز المخاطر التي تواجه مجال الشبكات اللاسلكية هو النهج القائم على رد الفعل الذي يفرضه التعقيد التشغيلي المستمر، حيث يقضي 63% من الكوادر معظم وقتهم في استكشاف الأخطاء وإصلاحها وإدارة الحوادث، ما يمنعهم من التركيز على العمل الاستباقي مثل المشاريع الاستراتيجية، والتدريب، والحصول على الشهادات، وتحسين أداء الشبكة.

إن هذا النمط التشغيلي القائم على "رد الفعل" يضعف جهود التحديث بشكل مباشر. فالفرق التي تعمل على استكشاف الأخطاء وإصلاحها تضطر لنقل مواردها واهتمامها بعيداً عن المسارات الحيوية الأخرى، مثل التخطيط الاستراتيجي للشبكات اللاسلكية، أو تطبيق تقنيات الأتمتة.

ويزيد من حدة هذا التحدي الافتقار إلى الرؤية الشاملة. إذ تشير 86% من المنظمات إلى وجود فجوات في القدرة على مراقبة الشبكة، ما يعيق فعالية استكشاف مشكلات شبكة الواي-فاي وحلها. وتشمل أبرز التحديات ضعف الرؤية الخاصة بالأجهزة المتصلة، ونقص الوضوح في أداء التطبيقات والخدمات السحابية، وضعف تتبع ومراقبة التجوال.

وفي غياب هذه الرؤية، تصبح الفرق غير قادرة على تحديد المشكلات بسرعة، ما يؤدي إلى معادلة صعبة وخطيرة: إذ تتحول الشبكات اللاسلكية في كثير من الأحيان إلى المتهم الأول لمشكلات تنشأ في أماكن أخرى. وقد أفاد 70% من المشاركين بأن أكثر من 10% من الحوادث تُنسب خطأً إلى الشبكات اللاسلكية.

في ظل التحول المؤسسي المتسارع المدعوم بالذكاء الاصطناعي، يتفق قادة مجال الشبكات اللاسلكية على أن الذكاء الاصطناعي يمثل الحل الأمثل للتغلب على هذه التعقيدات، لما يوفره من فوائد قابلة للقياس، بما في ذلك توفير الوقت، تبسيط العمليات، وتسريع حل المشكلات.

مع ذلك، لا يزال هناك فجوة كبيرة بين الواقع والتطلعات في تطبيق قدرات الذكاء الاصطناعي ضمن الشبكات اللاسلكية في المملكة العربية السعودية.

ويظل التعقيد التشغيلي وحده عائقاً رئيسياً أمام الاستفادة الكاملة من إمكانات الذكاء الاصطناعي وتحقيق أقصى عائد من الشبكات اللاسلكية. ومع تصاعد التهديدات السيبرانية - وهي العائق الثاني - يتفاقم هذا التحدي، ما يضاعف الضغوط على مرونة المنظمات ويؤثر سلباً في أدائها المالي.

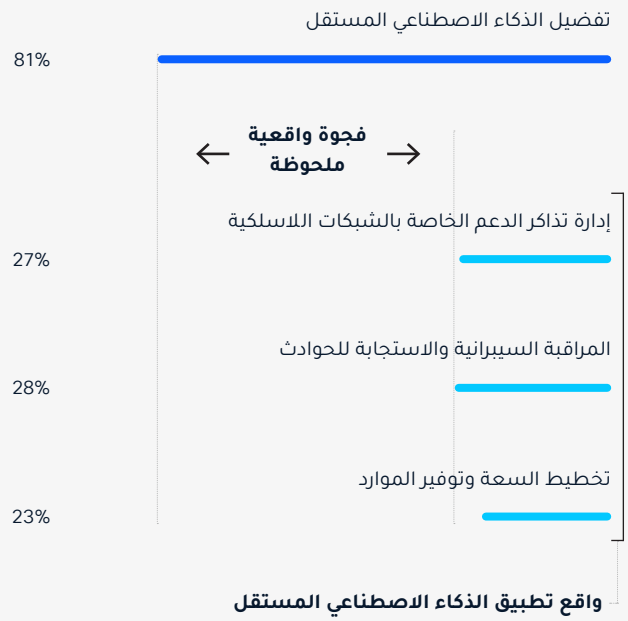
86% من المنظمات تواجه فجوات في وضوح الرؤية والرقابة، ومن أبرزها:

46% ضعف الرؤية الخاصة بالأجهزة المتصلة

42% نقص الوضوح في أداء التطبيقات والخدمات السحابية

37% ضعف تتبع ومراقبة التجوال

فجوة الذكاء الاصطناعي: الواقع والطموح



العائق الثاني: أمن الشبكات اللاسلكية في مواجهة التحديات - حين يلتقي توسّع أجهزة إنترنت الأشياء بتهديدات مدعومة بالذكاء الاصطناعي

يمثل أمن الشبكات اللاسلكية العائق الجوهري الثاني الذي يحدّ من قدرة المنظمات في المملكة العربية السعودية على تجاوز "مفارقة الذكاء الاصطناعي" وتحقيق عوائد قوية من استثماراتها في الشبكات اللاسلكية. ففي ظل التوسع المتسارع لأجهزة إنترنت الأشياء وتصاعد التهديدات السيبرانية المدعومة بالذكاء الاصطناعي، يصبح من الصعب على المنظمات الاعتماد بثقة على شبكة الواي-فاي كمنصة لتنفيذ العمليات التشغيلية المهمة، خاصة مع تزايد الخسائر المالية المرتبطة بالاختراقات السيبرانية وما تشكله من مخاطر مباشرة على استقرار الأعمال واستمراريتها.

تعرّضت 84% من المنظمات في المملكة العربية السعودية لحادثة أمنية واحدة على الأقل في الشبكة اللاسلكية خلال العام الماضي. كما أفادت 42% من هذه المنظمات بارتفاع مستوى التهديدات المرتبطة بالشبكات اللاسلكية خلال العامين الماضيين، مؤكدةً أنها أصبحت أكثر تواتراً وتعقيداً وخطورة، فضلاً عن صعوبة متزايدة في اكتشافها والتصدي لها.

تُعدّ الهجمات السيبرانية المُولّدة بالذكاء الاصطناعي أو المؤتمتة إحدى أبرز ثلاثة عوامل تساهم في تصاعد التهديدات السيبرانية التي تستهدف الشبكات اللاسلكية، فهي قادرة على رصد نقاط ضعف الشبكة بدقة، وتكييف أساليب الهجوم استجابةً لآليات الدفاع، مع العمل بسرعة ونطاق يفوقان بمراحل قدرات المهاجمين البشريين. لقد أحدث الذكاء الاصطناعي تحولاً جذرياً في سهولة اختراق شبكات الواي-فاي، إذ مكن المهاجمين من تنفيذ عمليات أكثر تطوراً وسرعة، وبموارد أقل بكثير مما كان يتطلبه الأمر في السابق.

تشهد المنظمات في المملكة العربية السعودية توسعاً مستمراً في مساحة الهجمات الإلكترونية التي تواجهها. فقد أفاد 35% من المتضررين من الحوادث السيبرانية بأن أنظمتهم تعرّضت للاختراق نتيجة استهداف أجهزة إنترنت الأشياء أو أجهزة التشغيل. ويُشكل ذلك تهديداً كبيراً لشبكات الواي-فاي، باعتبارها تقنية الاتصال الأكثر انتشاراً في بيئات إنترنت الأشياء. كما أن الانتشار المتزايد لأجهزة إنترنت الأشياء - خاصة عند غياب إدارتها أو تأمينها بشكل كافٍ - يؤدي إلى تراكم نقاط الضعف، حيث يمكن أن تتحول الثغرات الفردية إلى منفذ أمني واسع يهدد الشبكة بأكملها.

يمثل الأثر المالي للحوادث السيبرانية الخاصة بالشبكات اللاسلكية عبئاً كبيراً على المنظمات. فقد تكبدت 60% من المنظمات في المملكة العربية السعودية خسائر مالية نتيجة لحوادث أمنية متعلقة بالشبكات اللاسلكية. كما أفادت 51% من هذه المنظمات بأن خسائرها تجاوزت مليون دولار أمريكي خلال العام الماضي، وهو تأثير مالي كبير يبرز بوضوح أهمية الاستثمار في تعزيز أمن شبكات الواي-فاي.

لا تقتصر خسائر المنظمات في المملكة العربية السعودية جراء حوادث أمن الشبكات اللاسلكية على الجانب المالي فقط. فقد أفادت 35% من المنظمات بتراجع ثقة عملائها نتيجة لهذه الحوادث، بينما واجهت 37% منها عقوبات تنظيمية أو تبعات مرتبطة بالامتثال للقانون. ويؤكد ذلك أن تداعيات هذه الحوادث تتجاوز بكثير التكاليف المباشرة، لتشمل تأثيرات أوسع تمس السمعة المؤسسية والالتزامات التنظيمية.

ومع ذلك، لا تزال غالبية المنظمات تثق بأمن شبكاتها اللاسلكية، إذ أفاد 88% منها بأن جهود شركاتهم كافية لحماية هذه الشبكات، رغم أن 81% تتوقع في الوقت نفسه ارتفاع حالات اختراق أو فشل أمن الشبكات اللاسلكية خلال العامين المقبلين.

تشير المنظمات إلى ثلاثة عوائق رئيسية أمام تعزيز أمن الشبكات اللاسلكية: تعقيد التنفيذ، البنية التحتية القديمة، ومخاوف الأداء. ولا تعمل هذه العوائق بمعزل عن بعضها، بل تمثل جزءاً من تحديات أوسع تواجه الشبكات اللاسلكية، مثل نقص الكفاءات، محدودية الرؤية والشفافية، وتزايد الضغوط التشغيلية، ما يقيد قدرة المنظمات على تحديث وتحسين أمن شبكاتها بشكل فعّال.

والنتيجة هي اتساع فجوة الثغرات السيبرانية: فمع تصاعد المخاطر، تظل المنظمات مقيدة بالبنية التحتية القديمة، وتعقيد العمليات، ومخاوف الأداء، ما يعيق جهود التحول ويضعف قدرتها على الصمود أمام التهديدات المتزايدة.

مع ذلك، تُظهر نتائج هذا البحث أن المنظمات التي تعتمد أنظمة المصادقة الحديثة، سواءً القائمة على الشهادات أو المعرفات الرقمية، تحقق مستويات أعلى من الأمان، وأداءً مؤسسياً أفضل من المنظمات التي لا تستخدم هذه الأنظمة. كما تسجّل هذه المنظمات متوسط خسائر مالية أقل بكثير نتيجة الحوادث السيبرانية، مما يعزز قيمة الاستثمار في بروتوكولات المصادقة المتقدمة.

مع ذلك، يتطلب تطبيق بروتوكولات الأمان الحديثة خبرات متخصصة يصعب العثور عليها في سوق العمل اليوم. وهذا يقودنا إلى العائق الثالث: المنافسة على الكفاءات في مجال الشبكات اللاسلكية.

العوامل الرئيسية المساهمة في زيادة المخاطر على الشبكات اللاسلكية

التوسع المتسارع في استخدام إنترنت الأشياء والأجهزة المتصلة (نمو سريع في أعداد الأجهزة المتصلة بالشبكة)	32%
قيود الميزانيات أو الموارد تعيق تطوير وتعزيز القدرات السيبرانية	32%
نقص الكفاءات المتخصصة أو محدودية القدرة على رصد التهديدات والاستجابة لها	31%
الهجمات الإلكترونية المُولّدة بواسطة الذكاء الاصطناعي أو المؤتمتة وأدوات الاختراق المؤتمتة	27%
توسع نماذج العمل عن بُعد والهجين: اتساع رقعة الهجوم وتعدد الأجهزة الطرفية غير المُدارة	25%

العائق الثالث: الشبكات اللاسلكية تخسر المنافسة على كفاءات الذكاء الاصطناعي

يمثل نقص الكفاءات العائق الثالث، ويعدّ مع تعقيد العمليات وتصاعد التهديدات السيبرانية أحد العوامل الأساسية التي تحدّ من قدرة المنظمات على تحقيق عائد استثمار مجزٍ في مجال الشبكات اللاسلكية.

ولا يقتصر تأثير هذا النقص على الحدّ من جهود التحديث فحسب، بل يزيد أيضاً الضغط التشغيلي والمخاطر السيبرانية، ويعيق تطبيق تقنيات الذكاء الاصطناعي في عمليات تكنولوجيا المعلومات. وينتج عن ذلك حلقة مفرغة: فالمنظمات التي تفتقر إلى الكفاءات تصبح أبطأ في التحديث، ما يؤدي إلى تصاعد التعقيد والمخاطر السيبرانية وارتفاع التكاليف، وهو ما يدفع أفضل الكفاءات إلى الانتقال لشركات أكثر تطوراً وحداثة.

أشارت 91% من المنظمات في المملكة العربية السعودية إلى أنها تواجه تحديات في التوظيف، إذ تميل الكفاءات في مجال تقنية المعلومات إلى الانخراط في مجالات تقنية أكثر جاذبية وانتشاراً، مثل الذكاء الاصطناعي والأمن السيبراني. ويساهم هذا النقص في اتساع فجوة المهارات، حيث تُظهر النتائج إلى أن 40% من المنظمات تشير إلى ارتفاع تكاليف التشغيل، و40% بانخفاض الروح المعنوية، و28% بتراجع الابتكار.

تبدو العلاقة بين نقص الكفاءات والنتائج السلبية في المملكة العربية السعودية واضحة جداً. فالمنظمات التي تواجه صعوبة كبيرة في توظيف الكفاءات المتخصصة في الشبكات اللاسلكية تقضي وقتاً أطول بكثير في مهام الاستجابة. ولا يقتصر تأثير هذا النقص على العمليات التشغيلية فحسب، بل تتحمل هذه المنظمات أيضاً تكاليف سنوية أعلى للحوادث السيبرانية مقارنة بالمنظمات التي لا تواجه تحديات في التوظيف.

تواجه المنظمات التي تعاني من صعوبات في التوظيف ونقص الكفاءات المعتمدة تحديات متزايدة، تشمل ارتفاع تكاليف التشغيل، زيادة المخاطر السيبرانية، انخفاض مستوى الأتمتة، وتراجع القدرة على التحديث. في المقابل، فإن المنظمات التي تستثمر مبكراً في تطوير الكفاءات والحصول على الشهادات المتخصصة تكسب ميزة تنافسية واضحة، لا سيما مع تصاعد التعقيد وتزايد أهمية المهارات المتقدمة لضمان الكفاءة التشغيلية، وذلك في ظل المنافسة المتصاعدة على استقطاب الكفاءات.

تكشف أزمة الكفاءات عن الترابط العميق لمفارقة الذكاء الاصطناعي في مجال الشبكات اللاسلكية. فبدون دمج الذكاء الاصطناعي في صميم العمليات، ستواصل المنظمات فقدانها للكفاءات المتخصصة. ومع نقص هذه الكفاءات، يصبح تنفيذ المشاريع الاستراتيجية، مثل تحديث أنظمة الأمن، أكثر صعوبة. وفي ظل غياب أنظمة أمنية متقدمة، ترتفع تكاليف الحوادث، ما يزيد من صعوبة الاستثمار في الكفاءات والتكنولوجيا على حدٍّ سواء.

يوضح هذا التفاعل المتراكم ضرورة تعامل المنظمات مع العوائق الثلاثة في الوقت نفسه لضمان تجاوز مفارقة الذكاء الاصطناعي في الشبكات اللاسلكية.

الذكاء الاصطناعي مساهم في هجرة الكفاءات ونقص المهارات المتخصصة في مجال الشبكات اللاسلكية

الأسباب الرئيسية لصعوبة توظيف الكفاءات في مجال الشبكات اللاسلكية

قلة المرشحين ذوي المهارات المتقدمة في الشبكات اللاسلكية أو المهارات المدمجة مع الذكاء الاصطناعي	64%
قيود الميزانية الداخلية أو تجميد التوظيف	42%
عملية توظيف مطولة أو اختناقات داخلية	39%

أبرز ثلاثة مجالات تساهم في استنزاف الكفاءات عن مجال الشبكات اللاسلكية

الذكاء الاصطناعي وتعلم الآلة	61%
الأمن السيبراني	50%
هندسة البرمجيات وتطوير التطبيقات	42%

المنهجية

شمل هذا البحث مقابلات مع 6,098 شركة في 30 سوقاً عالمياً، من بينها 106 شركات في المملكة العربية السعودية. أعدّت شركة Sandpiper Research & Insights هذا البحث في نوفمبر 2025.

نطاق البحث

بيانات المشاركين: أُجريت مقابلات مع 6,098 من صناع القرار والمتخصصين التقنيين في مجال الشبكات اللاسلكية في شركات تضم 250 موظفاً فأكثر. ويعمل 61٪ من المشاركين في شركات يصل حجم مبيعاتها السنوية إلى 100 مليون دولار أمريكي فأكثر.

الأمريكتان
22%

أوروبا والشرق الأوسط وأفريقيا
28%

آسيا والمحيط الهادئ
50%

التغطية الجغرافية: شمل البحث 30 سوقاً عالمياً، من بينها: أستراليا، البرازيل، كندا، بر الصين الرئيسي، فرنسا، ألمانيا، هونغ كونغ، الهند، إندونيسيا، إيطاليا، اليابان، ماليزيا، المكسيك، هولندا، نيوزيلندا، الفلبين، بولندا، المملكة العربية السعودية، سنغافورة، جنوب إفريقيا، كوريا الجنوبية، إسبانيا، السويد، سويسرا، تايوان، تايلاند، الإمارات العربية المتحدة، المملكة المتحدة، الولايات المتحدة الأمريكية، وفيتنام.

المجالات المشمولة في البحث: شملت عينة المشاركين مجموعة واسعة من المجالات الحيوية، من أبرزها: خدمات الأعمال، البناء، التعليم، الهندسة، التصميم والهندسة المعمارية، الخدمات المالية، الخدمات الحكومية والعامة، الرعاية الصحية، التصنيع، الإعلام والاتصالات، الموارد الطبيعية، العقارات، خدمات المطاعم، تجارة التجزئة، خدمات التكنولوجيا، النقل، خدمات السفر وتجارة الجملة.

تاريخ البحث: تم إجراء البحث في نوفمبر 2025.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**