FORRESTER®

تسليط الضوء على الأمن

دليل استراتيجية الخدمات السحابية المختلطة للمؤسسات

دراسة أجرتها شركة FORRESTER CONSULTING لصالح شركة IBM، سبتمبر 2019

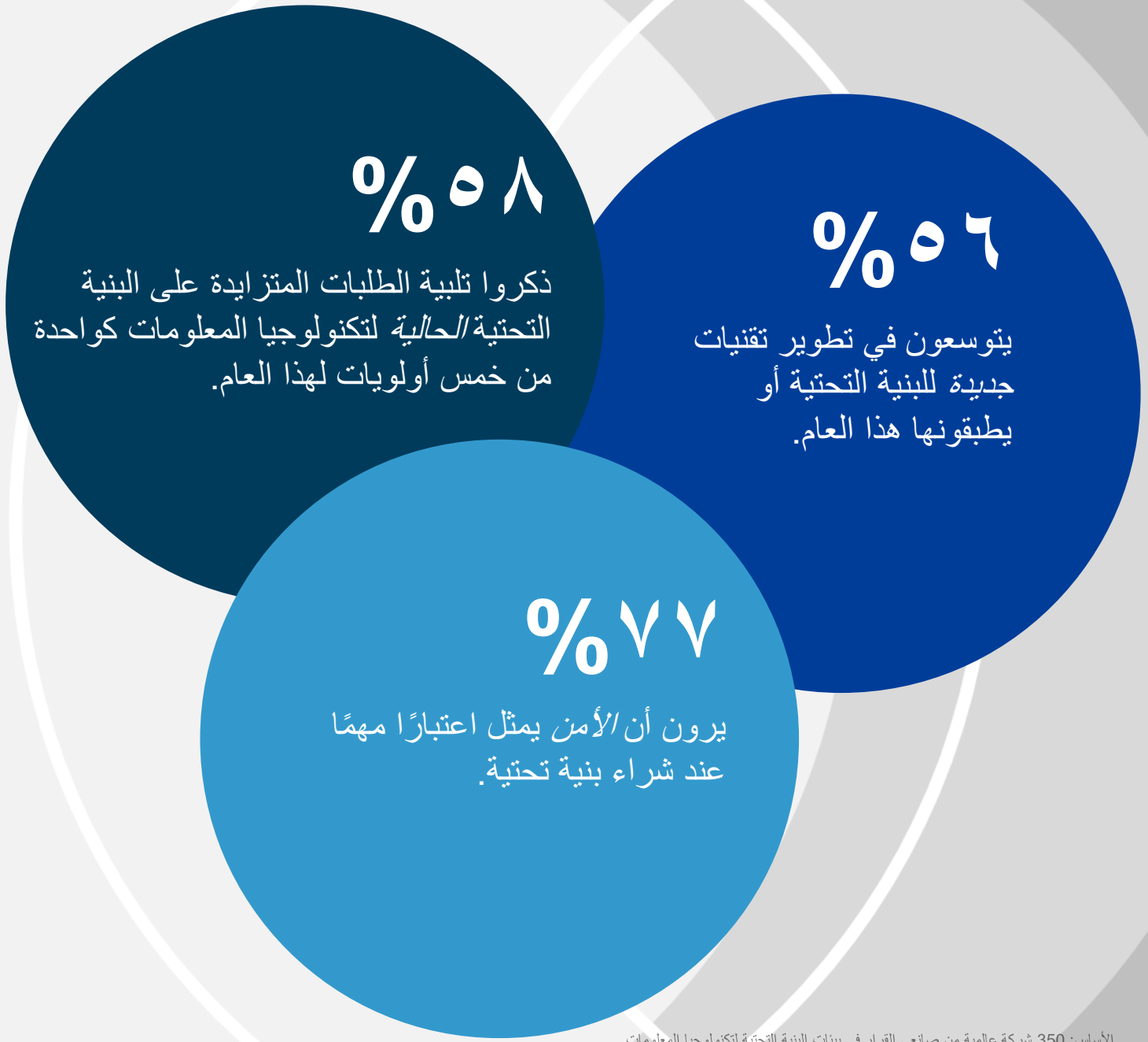
الموجز التنفيذي

ستصبح مؤسسات تكنولوجيا المعلومات الحديثة التي تتبنى نظرة شاملة للبنية التحتية لتكنولوجيا المعلومات لديها، بما في ذلك النماذج المحلية والنماذج السحابية، في وضع أفضل لمكافحة الثغرات الأمنية. تواجه المؤسسات اليوم حالة من عدم اليقين أكثر من أي وقت مضى. ومع تزايد التهديدات الإلكترونية من حيث العدد والتعقيد، أصبحت الحاجة إلى وجود بيئة رقمية آمنة أمرًا بالغ الأهمية. تحاول المؤسسات بدورها أن تعدِّل من استراتيجياتها للبنية التحتية لتقديم أفضل دعم لعملائها مع مواكبة أعباء الأعمال المعقَّدة، دون التضحية بالأمن.

في يناير ٢٠٢٠، نشرت شركة IBM دراسة أجرتها شركة Forrester Consulting لصالحها في سبتمبر ٢٠١٩ لتقييم كيفية تطوير المؤسسات وتنفيذها لاستراتيجياتها للبنية التحتية لتكنولوجيا المعلومات. أجرت شركة Forrester استطلاعًا عبر الإنترنت لعدد ٣٥٠ شركة عالمية من صانعي القرار في مجال تكنولوجيا المعلومات بمختلف الصناعات لاستكشاف هذا الموضوع. وجدنا أن المؤسسات تقوم بإنشاء بيئات سحابية مختلطة باستخدام مختلف الخدمات السحابية العامة، والخدمات السحابية الخاصة المستضافة، والبنى التحتية المحلية.

تخصِّص شركات تكنولوجيا المعلومات استثمارات ضخمة للبنية التحتية بغرض التغلُّب على التحديات الأمنية في الحاضر والمستقبل.

لا تركز المؤسسات على تلبية الطلبات المتزايدة على البنية التحتية لتكنولوجيا المعلومات الحالية فحسب، بل تركز أيضًا على ضمان الأمن في حين التوسع في التقنيات الجديدة.



الأساس: 350 شركة عالمية من صانعي القرار في بيئات البنية التحتية لتكنولوجيا المعلومات
المصدر: دراسة أجرتها شركة Forrester Consulting لصالح شركة IBM، سبتمبر 2019

في أوقات عدم اليقين، ومع أعباء العمل المتزايدة والمتغيرة، يجب على مؤسسات تكنولوجيا المعلومات تناول مسألة الأمن بشكلٍ شامل عند تعديل بنياتها التحتية.

تعزيز الأمن لمواجهة عدم اليقين عن طريق تحديث استراتيجية البنية التحتية لدى شركتك:

- تحديث استراتيجيتك باستمرار للحماية من الثغرات الأمنية
- المحافظة على البنية التحتية المحلية كعامل رئيسي في استراتيجية الأمن الشاملة لديك
- الاستفادة من البنية التحتية المحلية لتحسين قدرة الأمن على مواكبة أعباء العمل والتطبيقات الهامة

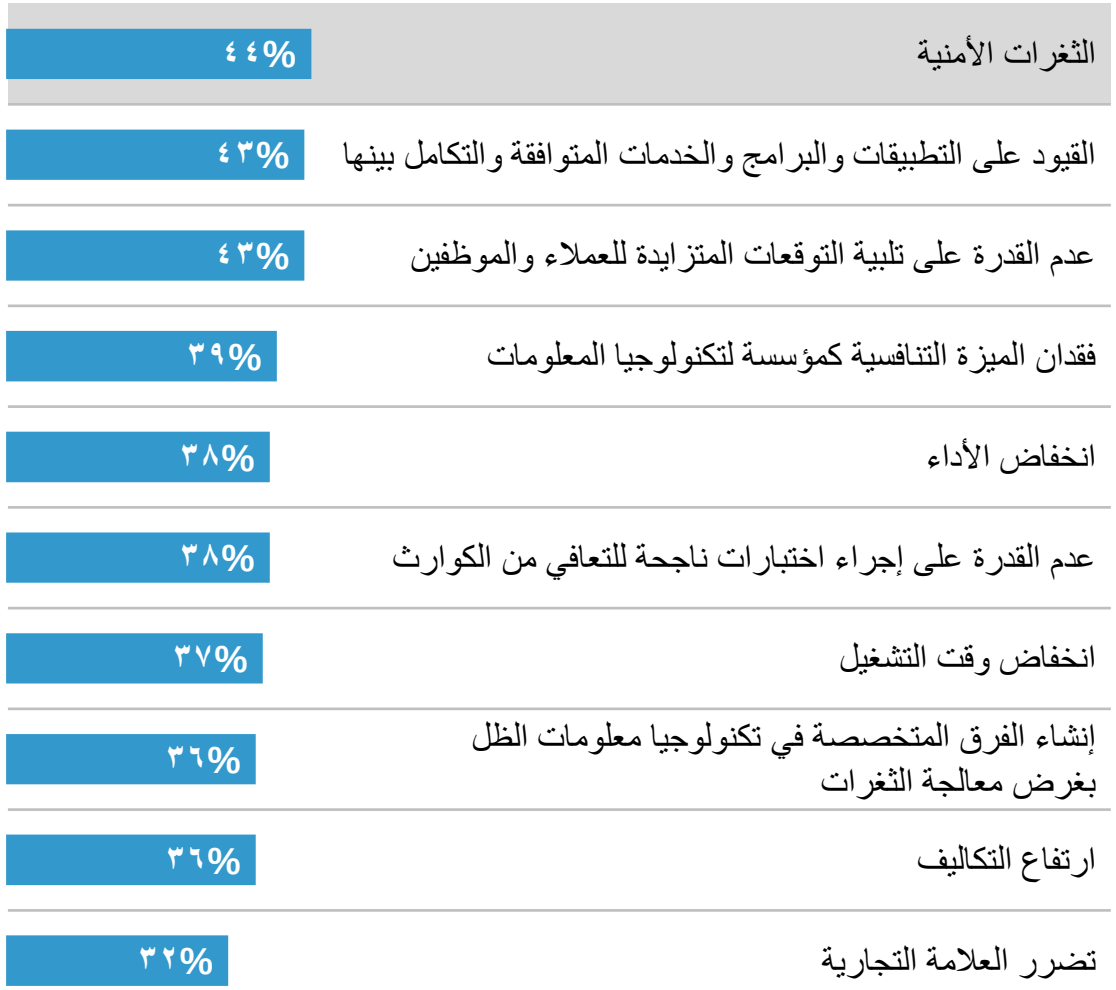
يؤدي عدم مواكبة تحديثات البنية التحتية إلى ظهور تهديدات

٦١% قاموا بتأخير تحديث البنية التحتية عدة مرات أو أكثر في السنوات الخمسة الماضية.

٣٨% من صانعي القرار يقولون إن شركاتهم واجهت فشلًا في اختبارات التعافي من الكوارث بعد تأخير التحديث.

أهم مخاطر التأخر في تحديث البنية التحتية

(معروض أهم ١٠ مخاطر، مصنَّفة من ١ إلى ٥)



الأساس: مختلف الشركات العالمية من صانعي القرار في بيئات البنية التحتية لتكنولوجيا المعلومات
المصدر: دراسة أجرتها شركة Forrester Consulting لصالح شركة IBM، سبتمبر 2019

المحافظة على البنية التحتية المحلية كعامل رئيسي في استراتيجية الأمن الشاملة لديك

تواصل الشركات التنويع في بنيتها التحتية باستخدام الأنظمة الأساسية للخدمات السحابية الخاصة، بما في ذلك الأنظمة الأساسية للخدمات السحابية المحلية. تظل البنية التحتية المحلية أساسية وجزءًا مهمًا من استراتيجية الخدمات السحابية المختلطة التي تتميز بالأمن والمرونة.

٤٠%

يقولون إن فشل الخدمات السحابية العامة في تلبية **احتياجات الأمن** هو السبب الذي دفعهم للحفاظ على البنية التحتية خارج منصات الخدمات السحابية العامة.

١٠/٩

يوافقون على أن البنية التحتية المحلية هي جزء مهم من استراتيجيات الخدمات السحابية المختلطة في شركاتهم.

الأساس: 350 شركة عالمية من صانعي القرار في بيئات البنية التحتية لتكنولوجيا المعلومات
المصدر: دراسة أجرتها شركة Forrester Consulting لصالح شركة IBM، سبتمبر 2019

الاستفادة من البنية التحتية المحلية لتحسين قدرة الأمن على مواكبة أعباء العمل والتطبيقات الهامة

أهم الأسباب لاستخدام الموارد المحلية لغرض مواكبة أعباء العمل والتطبيقات المختارة:

١	٢	٣	٤
ضمان أكبر للامتثال	الحد من التكاليف والثغرات الأمنية التي تتعرض لها البيانات أثناء النقل	تحسين أداء التطبيق/البنية التحتية	خفض التكاليف
٤٥%	٤٤%	٤٣%	٤٢%

الأساس: 241 شركة من صانعي القرار في مجال تكنولوجيا المعلومات يستخدمون حاليًا الخدمات السحابية العامة
المصدر: دراسة أجرتها شركة Forrester Consulting لصالح شركة IBM، سبتمبر 2019

التوصيات الرئيسية

إعطاء الأولوية لتحديثات البنية التحتية. ضع استراتيجية بنية تحتية واضحة وشاملة تستوعب بشكلٍ متواصل أعباء العمل المحلية وتركز على المشكلات الأمنية كمحرك أساسي لقرارات التحديث يجب على الشركات، حتى الشركات التي تكافح من أجل البقاء في ظل الوباء، أن تجعل تحديث البنية التحتية المتعلقة بالأمن أولوية قصوى.

وضع استراتيجية بيانات للإبلاغ عن القرارات المتعلقة بأعباء العمل؛ لتعزيز الأمن والأداء. تجنَّب الوقوع في فخ التفكير في التكاليف فقط عند اتخاذ القرارات المتعلقة بأعباء العمل. احتفظ بتأثير موقع البيانات في أعلى القائمة، بحيث تضبط الأداء العام بناءً على إدارة كلٍّ من مشكلات الأمان ووقت الاستجابة من خلال البيانات وأعباء العمل الكبيرة ذات الصلة على المنصة نفسها.

بناء دراسة جدوى لا تقبل الجدل. يُعد الأداء أمرًا بالغ الأهمية بشكلٍ خاص لما له من تأثير كبير على تجربة العملاء (CX) وتصوُّر العلامة التجارية. يمكن للمديرين التنفيذيين، ممن لا يستطيعون الالتزام بإكمال التحديثات، الاستفادة من خيارات تحديث البنية التحتية القائمة على الاشتراك، بحيث يكون التحديث أكثر مرونة في المستقبل حال تغيرت استراتيجيتهم.

المنهجية

في هذه الدراسة، أجرت شركة Forrester استطلاعًا عبر الإنترنت لعدد ٣٥٠ شركة عالمية من صانعي القرار في بيئات البنية التحتية لتكنولوجيا المعلومات لتقييم كيفية قيام المؤسسات بتطوير استراتيجياتها للبنية التحتية وتنفيذها. تضمَّن المشاركون في الاستطلاع صانعي القرار في مجال تكنولوجيا المعلومات في البنية التحتية والعمليات، أو إدارة التطبيقات أو صيانتها، أو تطوير البرمجيات. طُرحت على المشاركين أسئلة عن البيئات المستخدمة لأعباء العمل المختلفة والاستثمار في البنية التحتية. عُرض على المستجيبين حافزًا صغيرًا كنوع من الشكر على الوقت الذي أمضوه في الاستطلاع. بدأت الدراسة في أغسطس ٢٠١٩ واكتملت في سبتمبر ٢٠١٩.

مدير المشروع:
سينثيا هيكس،
مستشار تأثير السوق

المساهم في البحث:
المجموعة البحثية لمدير تكنولوجيا المعلومات في شركة Forrester

نبذة عن شركة FORRESTER CONSULTING

تقدِّم شركة Forrester Consulting استشارات قائمة على البحث تتميز بالموضوعية والاستقلال لمساعدة القادة على النجاح في مؤسساتهم. ويتراوح نطاق خدمات شركة Forrester Consulting الاستشارية من جلسات التخطيط القصيرة إلى المشروعات المخصصة، وتمكنك من الاتصال مباشرةً مع محلِّلي الأبحاث الذين يطبِّقون رؤيتهم كخبراء على التحديات التجارية المحدَّدة التي تواجهها. لمزيد من المعلومات، يُرجى زيارة forrester.com/consulting.