THALES

اتجاهات التشفير في الشرق الأوسط

2016

تسببت الخروقات والهجمات الإلكترونية بزيادة استعجال الشركات لتحسين الوضع الأمني وتبني استراتيجية تشفير مؤسسية وذلك على النحو المبين في الدراسة الاستطلاعية التي قمنا بإجرائها وشهدت مشاركة 368 من خبراء تكنولوجيا المعلومات والاتصالات في الشرق الأوسط

أهم النتائج

27 %

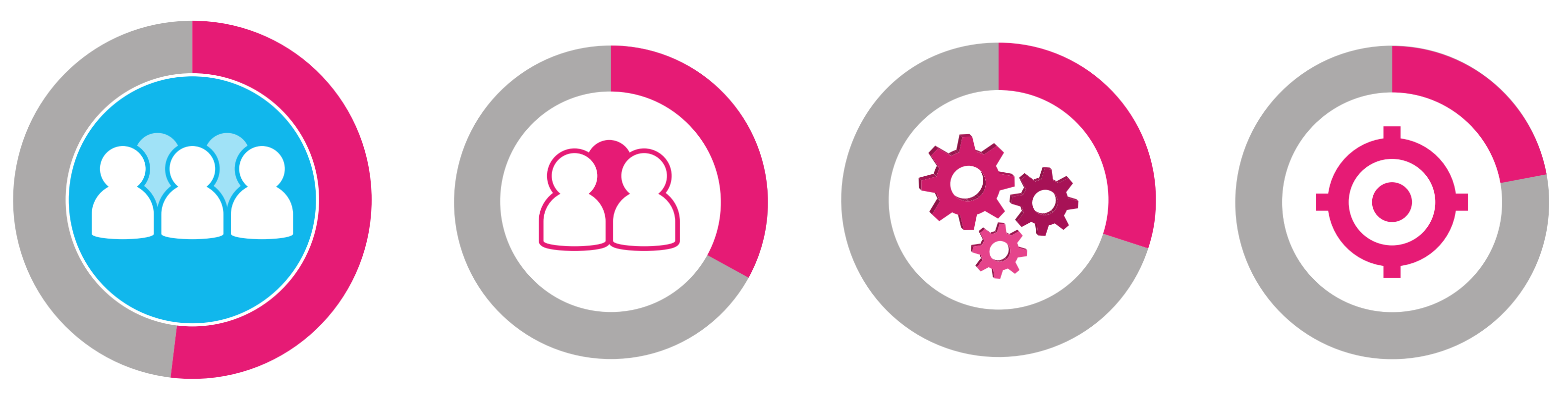
في جميع أنحاء المؤسسة

استراتيجيات التشفير المؤسسية

قال 27% فقط من المشاركين أن مؤسساتهم تمتلك استراتيجية تشفير مطبقة بشكل متسق في جميع أنحاء المؤسسة.

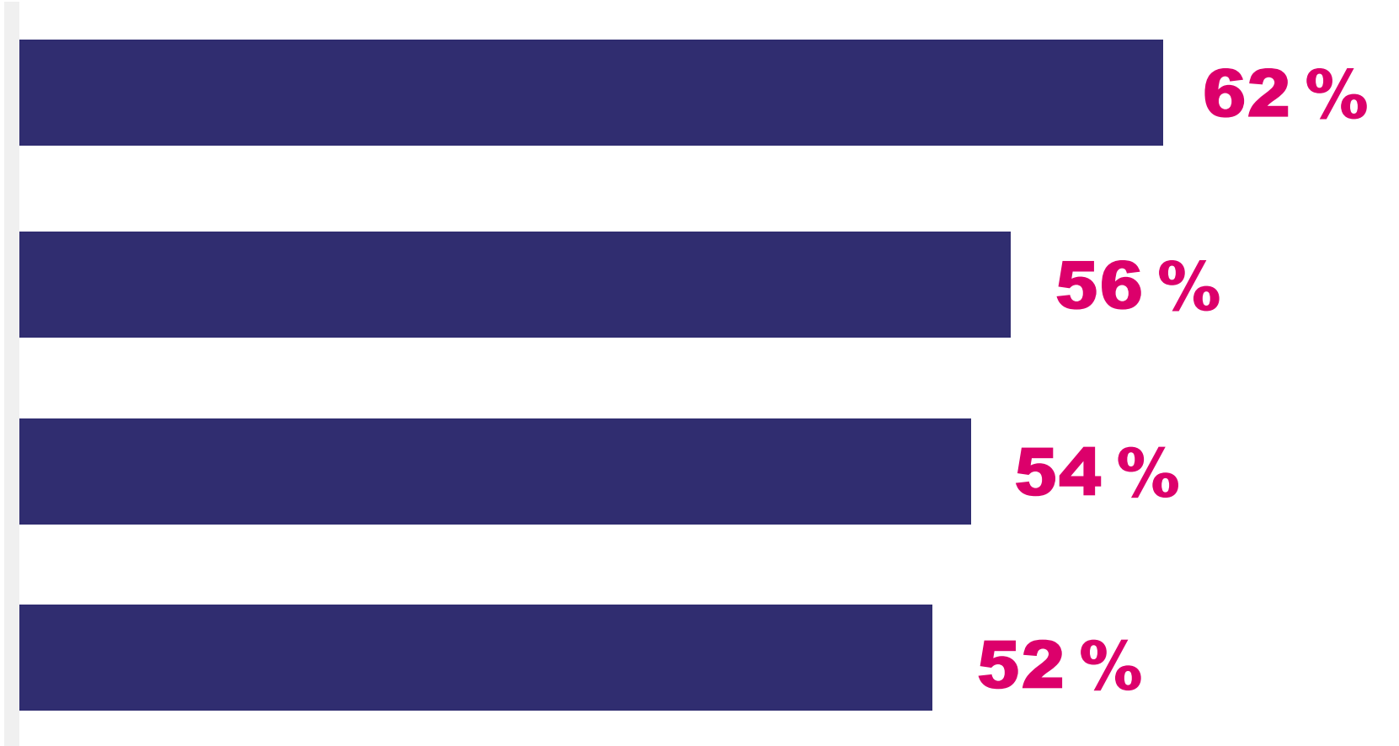
التهديدات

تشتمل قائمة أخطر التهديدات للبيانات الحساسة على:



23%	27%	35%	53%
القراصنة	مزودو الخدمات من الأطراف الثالثة	العمالة المتعاقدة	أخطاء الموظفين

ما هي الدوافع الرئيسية لاستخدام حلول تكنولوجيا التشفير؟



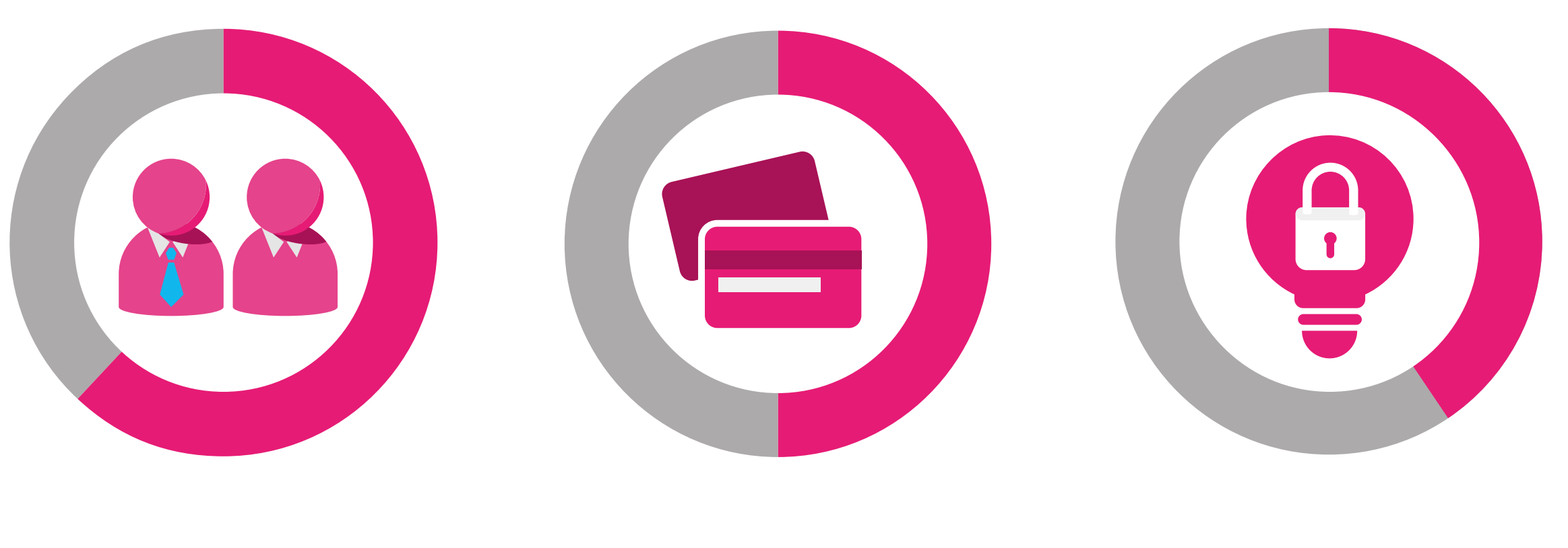
62 %	الالتزام باللوائح التنظيمية والمتطلبات الخارجية الخاصة بسياسة الخصوصية أو أمن البيانات
56 %	حماية معلومات العملاء الشخصية
54 %	حماية الملكية الفكرية الخاصة بالمؤسسة
52 %	حماية المعلومات من تهديدات محددة ومعروفة

التشفير

ما هي أبرز التحديات التي تواجه تطبيق استراتيجيات التشفير؟

استكشاف مكان تواجد البيانات الحساسة	54%
تطبيق تكنولوجيا التشفير كمرحلة أولية	39%
الإدارة المستمرة للتشفير والمفاتيح	35%

ما هي البيانات التي يتم تشفيرها في العادة؟



45 %	50 %	65 %
الملكية الفكرية	السجلات المالية	بيانات الموظفين/ الموارد البشرية

أي من القطاعات العالمية تستخدم تكنولوجيا التشفير؟

48 %	49 %	56 %
الخدمات	الصحة والأدوية	الخدمات المالية

ازدادت أهمية دعم تطبيق استراتيجية التشفير في كل من السحابة وداخل المؤسسة مع قيام الشركات بتبني حلول الحوسبة السحابية بصورة متزايدة وبحثها عن الاتساق ضمن جميع أنماط الحوسبة.

40 % 42 %

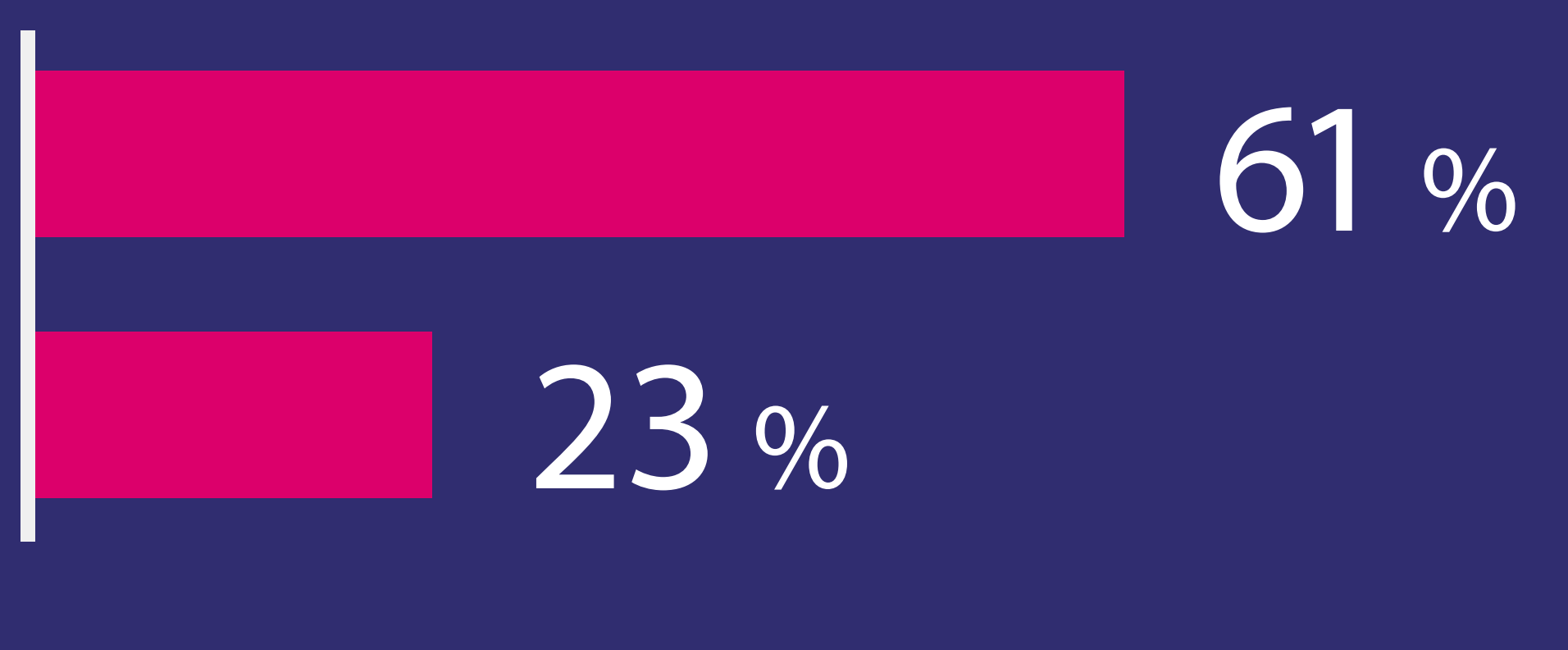
هل تكون البيانات بمأمن إذا ما تواجدت في السحابة وتمت حمايتها بواسطة تكنولوجيا التشفير؟

50%

تقوم 50% من المؤسسات بنقل البيانات الحساسة إلى السحابة في حال كانت أو لم تكن مشفرة أو تم جعلها غير قابلة للقراءة باستخدام آليات أخرى كالعملة الرقمة الرمزية أو إخفاء البيانات

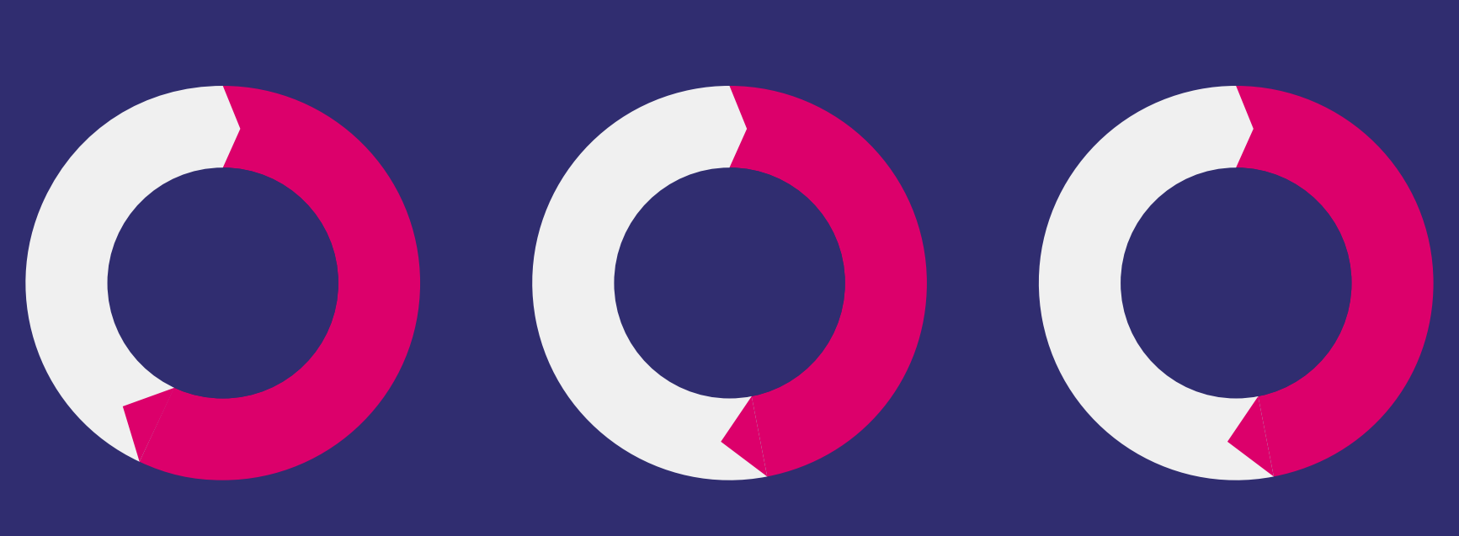
إدارة المفاتيح

لا تزال نسبة 61% من المؤسسات تستخدم العمليات اليدوية في حين تستخدم 23% منها الوسائط القابلة للإزالة المعرضة للتلف أو الفقدان



61 %	استخدام العمليات اليدوية يؤدي لحدوث الأخطاء
23 %	استخدام الوسائط القابلة للإزالة

ما الذي يجعل إدارة المفاتيح أمراً مزعجاً؟



46%	46 %	64 %
قلة أعداد الموظفين المهرة	أدوات إدارة المفاتيح غير الملائمة	عدم وجود ملكية واضحة

62 %

بلغت مستويات الإزعاج والمخاطر المرتبطة بإدارة المفاتيح في جميع الدول نسبة 53%، أعلاها في الشرق الأوسط بنسبة 62%، وأدناها في روسيا بنسبة 43%.

ستزداد أهمية وحدات أمن الأجهزة (HSMs) بالنسبة للتشفير أو إدارة المفاتيح خلال الأشهر الـ 12 القادمة

أبرز 5 حالات استخدام

22 %	23 %	24 %	24 %	29 %
تشفير السحابة العامة	توقيع المستندات	مصادقة أجهزة إنترنت الأشياء	تشفير قواعد البيانات	طبقة المنافذ الآمنة/أمن طبقة النقل (SSL/TLS)

تحميل الدراسة الكاملة

تابعونا على: