SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة

تأمين الاتصال التنظيمي في

المؤسسات الحكومية والتجارية والمجتمعية

جدول المحتويات

الملخص التنفيذي

لقد أدركت الحكومات في جميع أنحاء العالم التبعية الرقمية للصناعات المتطورة التي تمتد عبر الدفاع والرعاية الصحية والتمويل والطاقة. وفي الوقت الذي تواجه فيه هذه الصناعات تعقيدات العالم الرقمي، ظهر الاتصال الآمن والتعاون الفعّال كمعيار للتماسك التنظيمي والتعاون والامتثال. وعلى الرغم من أن التعاون الفعّال قد يعني أشياء مختلفة لشركات مختلفة بناءً على هيكلها التنظيمي أو تسلسلها الهرمي أو أهدافها، فإن الاتصال الآمن يوفر دائمًا نقطة تركيز واحدة للجميع، وهي حماية البيانات ومشاركة المعلومات دون تدخل وشبكات غير قابلة للاختراق تتصدى للهجمات الإلكترونية.

يمثل الاستقرار التنظيمي واستمرارية الأعمال وظيفةً مباشرةً للبنية التحتية الأمنية للشركة. وفي ظل المزيج المتنوع من العوامل الأساسية لضمان الأمان التنظيمي، يمثل الاتصال الآمِن بين فِرَق العمل الداخلية والموظفين عاملًا محوريًّا بإمكانه تحقيق تغيير جذري. ومع انتشار التهديدات الداخلية التي تشمل إهمال الموظفين والنوايا الخبيثة، تدرك المؤسسات الضرورة التي لا غنى عنها للرسائل الآمنة ومشاركة الملفات وتبادل المعلومات عبر شبكاتها الداخلية.

يتواصل ما يقرب من 91٪ من موظفي المؤسسة مع الزملاء أو العملاء أو الشركاء خارج ساعات العمل العادية. [5] ويمثّل استخدام برامج أو تطبيقات الطرف الثالث غير المصرَّح بها لهذه الاتصالات، خاصةً تلك التي تتضمن تبادل البيانات أو المعلومات الحساسة، مصدر قلق كبير. نقيّم في هذه الورقة الفنية، الطرق التي يمكن للشركات من خلالها تأمين شبكات الاتصالات الخاصة بها، والحفاظ على سيطرتها على بياناتها، وضمان إطار عمل متماسك، إذ تكون البيانات والمعلومات تحت حماية مضمونة. وتسلّط الوثيقة الضوء على المستويات المقلقة لنقاط الضعف في اتصالات المؤسسة، ما يجعل من الضروري نشر تقنيات المراسلة الآمنة ومنصات الحماية من تسرب البيانات.

المقدمة

يشكل التحوّل الرقمي أساس المؤسسات الحديثة، ما يتسبَّب في تحولات ملحوظة في طريقة تواصل المؤسسات مع أصحاب المصلحة الخارجيين والفِرَق الداخلية. ونظرًا لأن الشركات تبذل جهودًا معقولةً لتأمين قنوات الاتصال الخاصة بها الممتدة خارجها، فمن الضروري بالقدر نفسه بناء مسار اتصال قوي وآمن للاتصال الداخلي.

الاتصالات التنظيمية غير الخاضعة للرقابة من العوامل الرئيسة التي تعطِّل الأعمال

كانت الهجمات الإلكترونية أو حالات اختراق البيانات، الناتجة عن التهديدات التنظيمية الداخلية أو الداخلية، هي الأكثر تكلفةً في عام 2023. [1]

تحدث 56% من الهجمات الإلكترونية بسبب إهمال الموظف أو المتعاقد، ما يؤثر بشكل كبير على أهداف العمل. [2]

متوسط التكلفة لكل حادث ناتج عن الإهمال الداخلي، مثل استخدام أجهزة أو تطبيقات غير آمنة وخرق سياسة أمن الشركة، 484,931 دولارًا. [2]

تأمين الاتصالات الداخلية

شرط أساسي للحفاظ على نزاهة الأعمال

مع مواجهة المؤسسات للجانب الآخر لوضع الأعمال الرقمية التي يزداد انتشارها، يتعيَّن على الشركات الحديثة اعتماد نهج شامل ومحكَم ومشفَّر للاتصالات الحساسة وخصوصية البيانات

تحكم أفضل في البيانات

إنَّ استخدام نظام أساسي خاص بالمؤسسة يتجاوز التشفير الشامل ليشمل التحكُّم في الوصول المستند إلى الأدوار وسجلات البيانات ولوحات المعلومات يمكن أن يضمن حماية البيانات المترابطة ومنع سوء الاستخدام. [3]

إنتاجية الموظف وتركيزه

تتيح البوابة الآمنة والسلِسة والشامِلة للاتصال الجماعي بين الموظفين التعاون في الوظائف المختلفة، دون التعرُّض لخطر الاختراقات الأمنية أو مشكلة الاتصالات المجزَّأة.

الامتثال للوائح

يشكِّل تطبيق الدردشة المزود بتشفير منتظم تحديات كبيرة في المجالات الخاضعة للامتثال، مثل الحوكمة والتمويل. [4] وتحتاج هذه المجالات إلى منصات تجمع بين ميزات الأمان والضوابط الإدارية الرئيسة.

التشفير

تعزيز الوضع التنظيمي المترابط

على الرغم من الإجماع العام داخل الشركات على حماية البيانات الحساسة، فإن عدد كبير من المؤسسات لا تمارس الحذر في مشاركة البيانات والملفات. ويمكن أن يؤدي استخدام تطبيقات المستهلك التابعة لجهات خارجية، التي غالبًا لا تحتوي على التشفير بين الأطراف وضوابط الأمان المناسبة، إلى جعل المؤسسات عُرضةً لتهديدات أمنية كبيرة.

%70 من المديرين التنفيذيين للمؤسسات يعتبرون استخدام تطبيقات الطرف الثالث غير المصرَّح بها مصدر قلق بالغ

الكشف عن الجوهر الحقيقي للتشفير الشامل

يضمن تشفير البيانات والاتصالات النزاهة التنظيمية الشاملة من خلال توفير حالات استخدام متعدِّدة، مثل قادة الأعمال الذين يجرون بانتظام محادثات حسَّاسة، وفِرَق الاستجابة للحوادث التي تبحث عن مشاركة نشطة وآمنة للبيانات لاستمرارية الأعمال، والاتصال التنظيمي العام بين إدارات متعددة.

في عام 2023 بلغ متوسط التكاليف المترتبة على خرق البيانات 4.45 مليون دولار، وتم التوصل إلى أن ، التشفير هو أفضل وسيلة للحد من التكاليف*. [1]

كان متوسط التكاليف المترتبة على حالات الاختراق في المؤسسات التي تجري اتصالات مشفرة أقل بقيمة **221,593** دولارًا من متوسط التكاليف المترتبة على خرق البيانات البالغ **4.45 مليون** دولار[1]

*عوامل الحد من التكاليف هي عوامل مرتبطة بتكاليف أقل من المتوسط مترتبة على الخرق.

التشفير في عالم تتنوّع فيه لوائح معالجة البيانات

تنظّم قوانين مختلفة في مناطق جغرافية مختلفة عملية توليد البيانات وتخزينها ومعالجتها. وهذا يتطلّب الحاجة إلى مزيدٍ من السيادة الرقمية للمؤسسات التي ترغب في التحكُّم في بياناتها أثناء ممارسة حقوقها في استخدامها وتوزيعها. وقد برز التشفير باعتباره أحد عوامل التسهيل الرئيسة للسيادة الرقمية، ما أكسب ثقة العملاء وأصحاب المصلحة في حماية البيانات.

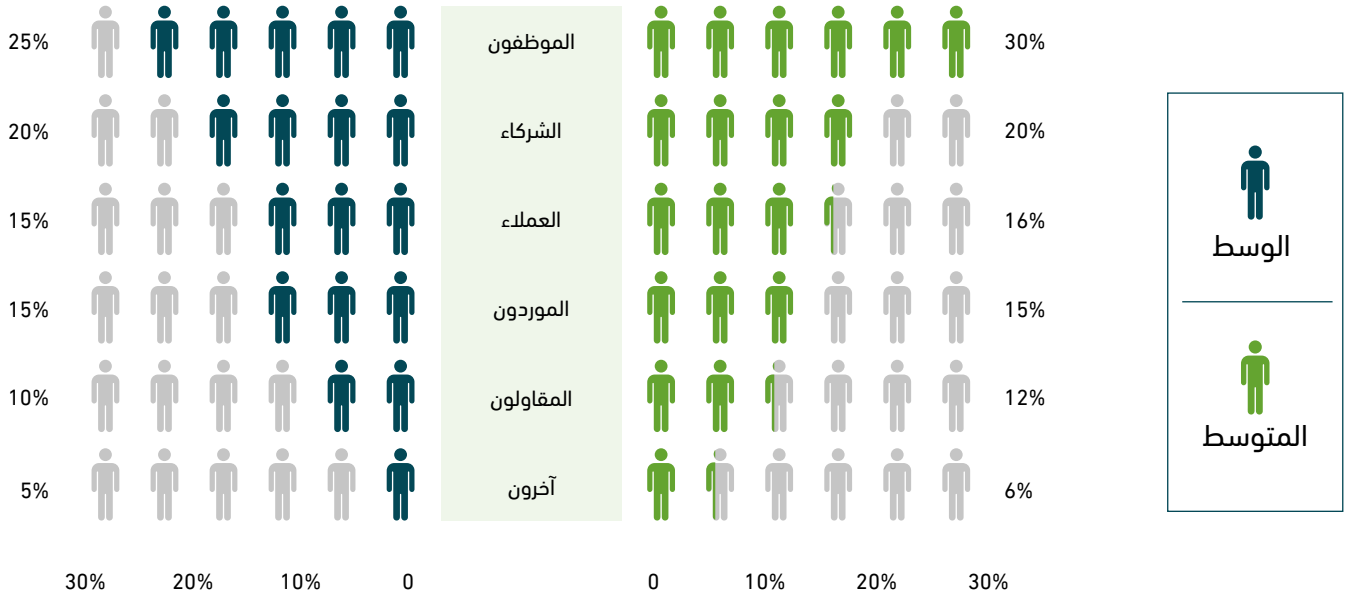
اعتبر 96% من المشاركين في استطلاع تقرير تهديدات البيانات التشفير الكامل وسيلةً مقبولةً لتحقيق سيادة البيانات. [6]

لماذا تعدُّ المراسلة الداخلية الآمنة ضرورة

تقييم وضع الضعف الأمني

تكشف المقارنة بين الأشخاص الذين يصلون إلى الموارد التنظيمية أنَّ الموظفين لديهم أعلى نسبة اختراق لموارد الشركة. وبالتالي تصبح أهمية ضمان وجود قنوات آمنة في هذا السيناريو للاتصال داخل المؤسسات أمرًا لا جدال فيه.

مجموعة واسعة من الأشخاص يصلون إلى الموارد [7]



إنَّ التخلص من استخدام تطبيقات الطرف الثالث غير المصرَّح بها، التي يُعارض استخدامها البروتوكولات التنظيمية ويجعل المعلومات الحسَّاسة عُرضةً للسرقة أو سوء الاستخدام، هو الخطوة الأولى في ضمان الاتصال الداخلي الآمن الشامل بين الفِرَق والموظفين.

أساسيات منصة المراسلة الآمنة للمؤسسات

حلول عبر القطاعات الصناعية المتعددة

يجب أن تكون حلول المراسلة الآمنة قابلةً للتوسُّع لتلبية احتياجات قطاعات مختلفة، سواء كان ذلك في القطاع الحكومي الذي يتطلب حماية المصالح الوطنية أو البنية التحتية الحيوية، أو في الشركات التي تحتاج إلى الحفاظ على استمراريتها.

الضوابط الإدارية

يتطلَّب منع استغلال البيانات نظامًا أساسيًّا شاملًا ومتماسكًا يسمح للمؤسسة بالتحكم في البرامج والأذونات ووحدات التحكُّم والاستضافة.

التهديدات الداخلية
منظور عالمي وإقليمي

يمكن للتهديدات الداخلية التي تشمل المستخدمين المصرَّح لهم مثل الموظفين أو الشركاء، الذين يعرضون البيانات للخطر أو يشنون هجمات إلكترونية أو يسهلون التجسُّس عن قصد أو عن غير قصد، أن تعرقل الأداء التنظيمي بشكل كبير. ويمكن أن تحدث هذه التهديدات نتيجة عدم الامتثال لسياسات أمن الشركة. تحدث 2 من أصل 3 تهديدات داخلية نتيجةً للإهمال أو عدم الامتثال للسياسات الأمنية. [8] لذلك، هناك حاجة إلى استخدام بروتوكولات اتصال قوية يمكنها ضمان الالتزام بسياسات أمن الشركة والقضاء دائمًا على الإهمال.

على مستوى العالم

86

متوسط عدد الأيام اللازمة لاحتواء الحادث الناتج عن مخاطر داخلية [9]

16.2مليون دولار لكل مؤسسة

متوسط التكلفة السنوية الناتجة عن مخاطر داخلية [9]

منطقة الشرق الأوسط وأفريقيا

15.4

متوسط الحوادث السنوية الناتجة عن إهمال الموظفين أو المقاولين في الشركات في الشرق الأوسط وأفريقيا. [2]

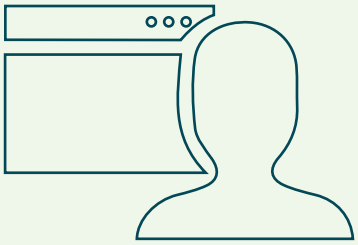
تواجه الشركات في الشرق الأوسط وأفريقيا معظم الحوادث الداخلية مقارنةً بأوروبا وآسيا والمحيط الهادئ وأمريكا الشمالية. [2]

المملكة العربية السعودية

نسبت 27% من الشركات السعودية الحوادث الإلكترونية التي تعرَّضت لها إلى سلوك ضار من الموظفين. [10]

تتطلب الاتصالات السريعة والمتعددة الجوانب بين الموظفين التعاون المتكامل

شبكة اتصالات الموظفين في كيانات الشركات [12]



متوسط عدد الأشخاص الذين يتصل بهم كل موظف في أسبوع العمل النموذجي.

37
زميل عمل

24
شريكًا

21
عميلًا

تأمين الفضاء الإلكتروني داخل القطاعات الرئيسية في المملكة العربية السعودية

في الوقت الذي تحقّق فيه المملكة العربية السعودية قفزات سريعة نحو تحقيق أهداف التحول الرقمي في إطار رؤية 2030، تركِّز المملكة بشكل كبير على حماية البنية التحتية الوطنية الحيوية في الجهات الحكومية والتجارية.

دور الهيئة الوطنية للأمن السيبراني في ضمان الأمن الشامل للبيانات والمعلومات.

استخدمت الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية ضوابط الأمن السيبراني للبيانات في المستويات الحكومية والمؤسسية لحماية الشبكات والأنظمة والبيانات السيبرانية. [12] وذلك لتحقيق الأهداف الاستراتيجية الرئيسة للهيئة.

حماية البيانات الوطنية

دعم الأمن السيبراني المؤسسي من خلال دورة حياة البيانات

ضمان التعامل الآمن مع البيانات

التدخل التكنولوجي لتأمين البنية التحتية الحيوية

تعدُّ القناة الآمنة للاتصال التنظيمي في المستويات الحكومية والتجارية والفردية أمرًا بالغ الأهمية لنجاح الاستراتيجية الوطنية للأمن السيبراني في المملكة العربية السعودية، وكذلك ضوابط الأمن السيبراني للبيانات. وتؤدي تقنيات منع تسرب البيانات التي تمنع الوصول المصرَّح به إلى المعلومات أو البيانات الحساسة أو استخدامها أو نقلها دورًا مهمًّا في تحقيق أهداف الاستراتيجية الوطنية للأمن السيبراني. وتكتسب هذه التقنيات أهميةً في الصناعات الرائدة، مثل الحوكمة والرعاية الصحية والدفاع والتمويل في جميع أنحاء المملكة العربية السعودية.

شركة الإلكترونيات المتقدمة إيان

تأمين الحكومة والمؤسسات والمجتمعات في المملكة العربية السعودية

شركة الإلكترونيات المتقدمة إيان هي منصة آمنة وذات سيادة ومستدامة تستخدم التشفير الشامل لحماية البيانات والمعلومات مع ضمان الامتثال للوائح التنظيمية.

آمنة
حماية ضد الوصول غير المصرَّح به أو الاعتراض

ذات سيادة
ضمان التحكُّم الشامل في البيانات للمؤسسات

مستدامة
انخفاض تخزين للبيانات مع عدم وجود انبعاثات

يمكن للمؤسسات السعودية، سواء كانت حكومية أو غير حكومية، مع شركة الإلكترونيات المتقدمة إيان، الالتزام بمتطلبات الأمن السيبراني الوطنية ومواجهة التحديات المتعلّقة بالاتصال الداخلي الآمن، كل ذلك أثناء السيطرة على مشاركة البيانات الخاصة بها واتباع لوائح الامتثال الخاصة بها.

تحقيق مؤشرات الأداء الرئيسة للاستراتيجية الوطنية للأمن السيبراني مع شركة الإلكترونيات المتقدمة إيان

تحدِّد الاستراتيجية الوطنية للأمن السيبراني ثلاثة مؤشرات أداء رئيسة لتقييم نجاحها في تحقيق الأهداف والغايات الأساسية. تعمل شركة الإلكترونيات المتقدمة إيان، من خلال بروتوكولات الاتصال الآمنة والمشفَّرة، على تسهيل الإنجاز الشامل لمؤشرات الأداء الرئيسة هذه.

تعزيز الثقة: تجمع شركة الإلكترونيات المتقدمة إيان بين الاتصال الخاص والتعاون الآمن عن طريق حماية البيانات الوصفية القوية. يمنح استخدام التشفير الشامل علامة ضمان للحكومات والمؤسسات ذات المهام الحرِجة التي يُطلَب منها باستمرار مشاركة بيانات ومعلومات حساسة. وهذا بدوره يخلق بيئةً من الثقة المتبادلة بين الموظفين والمؤسسات والشركات في المملكة العربية السعودية.

تقليل المخاطر: تضمن ميزات استضافة النظام المحلي على السحابة الخاصة التحكُّم في بياناتك ومنع استغلال البيانات. ويقلِّل ذلك من المخاطر الناتجة عن الهجمات الداخلية، سواء كانت من مُطّلعين خبيثين أو موظفين يتطلَّعون بشكل مقصود أو غير مقصود إلى إلحاق الضرر بنزاهة المؤسسة أو أمانها أو امتثالها للوائح والأنظمة. ومن خلال عناصر التحكُّم الإدارية مثل الدوائر الخاصة ومحو المحتوى تلقائيًّا وخزينة الملفات الآمنة، تساعدك شركة الإلكترونيات المتقدمة إيان على العمل بسلاسة في مساحة آمنة.

المساهمة في النمو: من خلال مجموعة الميزات التي تلبي احتياجات جميع المجموعات التنظيمية بما في ذلك الفِرَق والمستجيبين الأوائل والقادة، تسمح شركة الإلكترونيات المتقدمة إيان للجهات الحكومية ومؤسسات الأعمال بالتركيز على وظائفها الأساسية دون القلق بشأن المخاطر أو نقاط الضعف في الاتصالات غير الآمنة في تطبيقات الطرف الثالث، حيثُ إنها تدمج الاتصال الآمن بسلاسة مع ميزات القيمة المضافة التي تعزِّز الإنتاجية التنظيمية.

تحويل الاتصالات في جميع أنحاء المملكة: حالات الاستخدام الرئيسة

الارتقاء بريادة المملكة العربية السعودية

إدارة المحادثات الخاصة بأمان ومراقبة أنشطة الفريق في الوقت الفعلي لضمان استمرارية الأعمال.

تسهيل الاتصال في حالات الطوارئ

تمكين التعافي السريع من الكوارث مع الالتزام بمعايير أمن البيانات في المملكة العربية السعودية.

تعزيز الكفاءة

تحسين التنسيق بين المستجيبين الأوائل داخل المملكة. وسد فجوات الاتصال وتقديم المعلومات بسرعة للموظفين بدون مكاتب باستخدام أداة موثوقة.

منح فرص مميزة لمؤسستك

تحسين الثقة في أمن الموظفين **بنسبة 82٪** من خلال تطبيق شركة الإلكترونيات المتقدمة إيان البديهي، لإجراء مكالمات آمنة والدردشة والاجتماعات ومشاركة الملفات وتلقّي تحديثات الشركة تحت علامتك التجارية.

تحسن **بنسبة 58%** في الامتثال بوحدة تحكُّم إدارية سهلة الاستخدام لتنفيذ سياسات الاتصال التي تمتثل للوائح الخاصة بك.

سيادة البيانات **بنسبة 100٪** من خلال استضافة النظام المحلي، واستخدام العُقَد اللامركزية على سحابة خاصة أو محلية، بما يتماشى مع متطلباتك القضائية.

المراجع

1. IBM, 2023. Cost of a Data Breach Report 2023. Available at: https://www.ibm.com/reports/data-breach
2. Proofpoint, 2023. Cost of Insider Threats. Available at: https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats [Accessed 26 June 2024].
3. IBM, 2023. Understanding Role-Based Access Control (RBAC) for Log Analysis. Available at: https://www.ibm.com/support/pages/understanding-role-based-access-control-rbac-log-analysis
4. Forrester, 2023. Enable Secure Communications To Protect Data And Privacy. Available at: https://www.forrester.com/report/Enable-Secure-Communications-To-Protect-Data-And-Privacy/RES141180?utm_source=https%3A%2F%2Fjobalert.ie
5. NetSfere, 2023. Taking Control: How Secure Enterprise Messaging Puts Enterprise IT Back in Charge. Available at: https://www.netsfere.com/assets/Taking-Control-How-Secure-Enterprise-Messaging-Puts-Enterprise-IT-Back-in-Charge.pdf
6. IT Security Wire, 2023. Importance and Benefits of Data Encryption. Available at: https://itsecuritywire.com/featured/importance-and-benefits-of-data-encryption/
7. Thales Group, 2023. 2023 Data Threat Report. Available at: https://cpl.thalesgroup.com/data-threat-report
8. CyberSense, 2023. Insider Threats. Available at: https://cybersense.ai/applications/insider-threats
9. Ponemon Institute and DTEX, 2023. 2023 Cost of Insider Risks Global Report. Available at: https://www2.dtexsystems.com/l/464342/2023-09-15/3w7l7k/464342/1694800570ZwvyrzsD/2023_Cost_of_Insider_Risks_Global_Report___Ponemon_and_DTEX___Dgtl.pdf
10. Zawya, 2023. Insider Cyberthreats: 27% of Companies in Saudi Arabia Suffered from Malicious Actions by Staff. Available at: https://www.zawya.com/en/press-release/research-and-studies/insider-cyberthreats-27-of-companies-in-saudi-arabia-suffered-from-malicious-actions-by-staff-h2noolqd
11. Forrester, 2023. 217 Global Communications Technology Decision-Makers. Source: A commissioned study conducted by Forrester Consulting on behalf of Element, May 2023.
12. National Cybersecurity Authority, 2023. Controls List. Available at: https://nca.gov.sa/en/legislation?item=317&slug=controls-list

SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة

SAMI Advanced Electronics Company
King Khalid International Airport Industrial Estate
P.O. Box 90916,
Riyadh 11623, Saudi Arabia

+966112201350 **Email** - info@aecl.com

/AECSaudiArabia