cisco
آمن

مستقبل جدار الحماية

تحقيق وضعية أقوى اليوم مع بناء جسر لتلبية متطلبات الأعمال والأمان المستقبلية

جدول المحتويات

الملخص

يتمثل الغرض من هذا المستند التقني في مناقشة تطور أمان الشبكات وما سيتطلبه لحماية بيئة المؤسسة في المستقبل.

عندما تصبح الشبكات أكثر تباينًا، تزداد صعوبة تحقيق المؤسسات لإدارة السياسات المتسقة وتنفيذها والحفاظ على إمكانية رؤية موحدة. وغالبًا ما يؤدي تعقيد هذه الشبكات المترابطة إلى أخطاء أو عمليات تكوين خاطئة، الأمر الذي يجعلها عرضة للتهديدات المتطورة ودائمة التطور.

ما الذي يمكن للمؤسسة القيام به لاستعادة زمام التحكم وتحقيق الاتساق؟ تتمثل البداية في نهج متكامل للأمان يضع جدار الحماية في الواجهة وفي المركز.

ما يزال توزيع جدران الحماية بمثابة حجر الزاوية لاستراتيجية أمان الشبكة الخاصة بالمؤسسة، ولكن، مع تطور الشبكات، يجب أيضًا أن يتم تطوير توزيع جدران الحماية لدينا. فيما مضى، كان جدار الحماية جهازًا مفردًا عند "محيط" الدخول/الخروج يعمل كنقطة تحكم توجهها السياسة للسماح بحركة مرور بيانات الشبكة أو رفضها. لتحقيق النجاح في العالم الرقمي اليوم، تحتاج المؤسسات إلى التفكير فيما وراء توزيع جدران الحماية الفردية وتبني "توزيع جدران الحماية" - وهو أسلوب توجهه سياسة ما لتنسيق طبقات الحماية الأمنية المتقدمة بشكل استراتيجي عبر نقاط التحكم المنطقية على مستوى الشبكات غير المتجانسة بأكملها.

وسيكون تحديد توزيع جدران الحماية بمثابة خطوة مهمة للمؤسسات لمواءمة الأمان بشكل أفضل مع تغير احتياجات الأعمال والشبكات. لقد عملت Cisco جاهدة في العمل على إنشاء نظام أمان أساسي متكامل مع جدار الحماية الخاص بنا لدى المؤسسة لتمكين الشركات من تحقيق الانتقال.

> "ما تزال توزيع جدران الحماية بمثابة حجر الزاوية لاستراتيجية أمان الشبكة الخاصة بالمؤسسة، ولكن، مع تطور الشبكات، يجب أيضًا أن يتم تطوير توزيع جدران الحماية لدينا."

من خلال توزيع جدران الحماية، يمكن للمؤسسات التي تشهد تحولًا رقميًا تحقيق وضعية أمنية أقوى اليوم مع بناء جسر لتلبية متطلبات الأعمال والأمان المستقبلية.

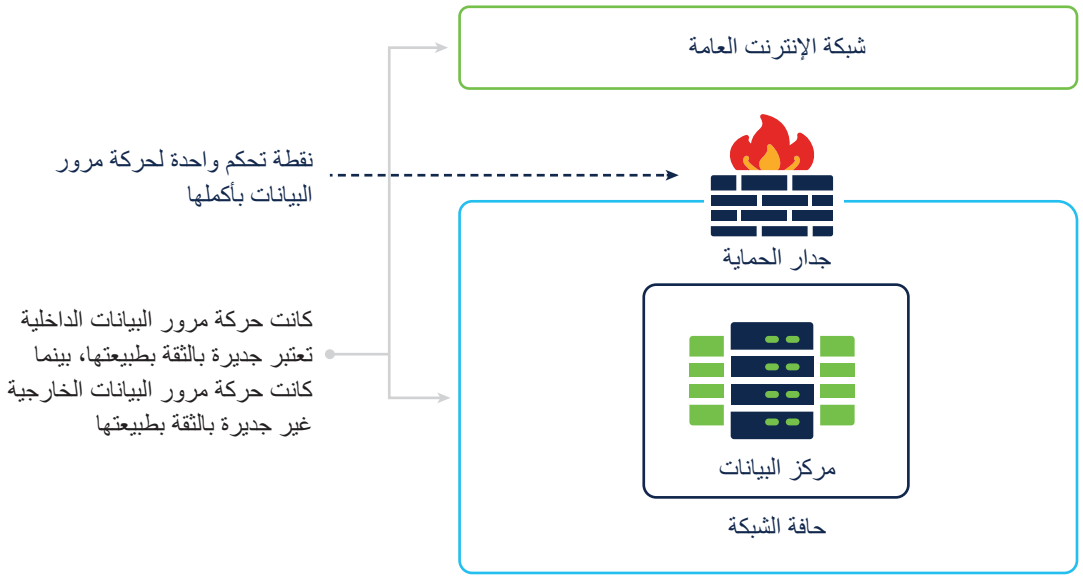
القسم 1: تاريخ جدار الحماية

تطور أمان الشبكة

وبشكل تقليدي، تم وضع جدار الحماية كحارس بوابة على حافة الشبكة. حيث كان يعمل كنقطة تحكم شاملة، تفحص حركة مرور بيانات الشبكة أثناء انتقالها عبر هذا المحيط. من خلال استقرار جدار الحماية عند نقطة الدخول/الخروج بالشبكة، فقد كان مسؤولًا عن التحقق من صحة الاتصالات: كانت حركة مرور بيانات الشبكة الداخلية تعتبر جديرة بالثقة بطبيعتها، بينما كانت حركة مرور البيانات الخارجية تعتبر غير جديرة بالثقة بطبيعتها. تم إنشاء مجموعات القواعد والسياسات وفرضها عند نقطة التحكم الأحادية هذه للتأكد من السماح لحركة مرور البيانات المطلوبة داخل الشبكة وخارجها ومنع حركة مرور البيانات غير المرغوب فيها.

بمقارنة محيط الشبكة بخندق حول قلعة، كان جدار الحماية بمثابة جسر متحرك يتحكم في حركة مرور البيانات بالكامل داخل الحصن وخارجه.

أمان الشبكة التقليدي



الشكل 1. نهج جدار حماية الشبكة التقليدي

على امتداد السحابة. والتطبيقات.

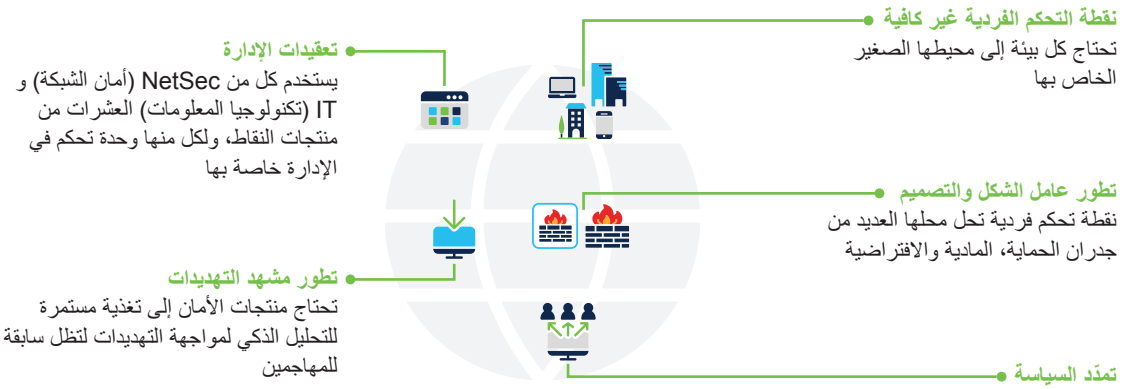
لم يمضِ وقت طويل قبل أن يتم التشكيك في هذه الممارسة المتمثلة في فرض الأمان من خلال نقطة تحكم واحدة. أولاً، برز في البداية مفهوم الوصول عن بعد وإمكانية التنقل على مستوى المؤسسة. ولكن التحول بدأ بالفعل مع ظهور الحوسبة السحابية. عندما انتقلت الأعمال إلى السحابة، بدأت الأجهزة والمستخدمون في الرحيل بشكل جماعي خارج الشبكة الداخلية الخاضعة للتحكم، مما جعل نموذج نقطة التحكم الواحدة غير فعال. عما قريب، أصبحت هناك العديد من الطبقات المحيطة. وكلها يتعين تأمينها. لم تكن هناك طريقة فعالة لوضع خندق واحد حول الشبكة.

واليوم، تعمل مواقع المكاتب الفرعية وعمل الموظفين عن بُعد والاستفادة المتزايدة من الخدمات السحابية على دفع مزيد من البيانات بعيدًا عن "المحيط" التقليدي، الأمر الذي يتجاوز فكرة نقطة التحكم التقليدية في الأمان بشكل كامل. بالإضافة إلى ذلك، تبنّت العديد من الشركات نموذج "إحضار جهازك الخاص (BYOD)"، مما يسمح للموظفين بالوصول إلى تطبيقات الأعمال الحساسة من خلال أجهزة الكمبيوتر الخاصة بهم أو أجهزتهم المحمولة. ففي الواقع، يستخدم أكثر من 67% من الموظفين أجهزتهم الخاصة في العمل - وهو اتجاه تصاعدي بلا نهاية في الأفق. والأجهزة المحمولة وأجهزة الكمبيوتر المحمولة المتصلة عبر شبكات Wi-Fi القابلة للوصول إليها للعامة هي السائدة، حتى وإن كانت ذات أهمية في عمليات الأعمال اليومية.

علاوةً على ذلك، فإن الغالبية العظمى من مواقع الأعمال والمستخدمين يحتاجون أيضًا إلى الوصول المباشر إلى الإنترنت حيث توجد الآن أغلبية متزايدة من التطبيقات والبيانات المهمة القائمة على السحابة. وتستمر الشركات في نشر أعباء العمل عبر الخدمات السحابية المتعددة، وأنظمة التشغيل، والأجهزة المادية، وقواعد البيانات، والمزيد. تصبح التطبيقات والبيانات لامركزية بدرجة أكبر، بينما تصبح الشبكات بالتالي أكثر تنوعًا.

الواقع الجديد

لقد أثبت هذا النهج، "حجم واحد يناسب الجميع"، أنه غير فعال في المشهد المعاصر.



الشكل 2. تعقيد الشبكة والتهديدات المتطورة يمثلان صعوبة تواجه نموذج جدار الحماية التقليدي

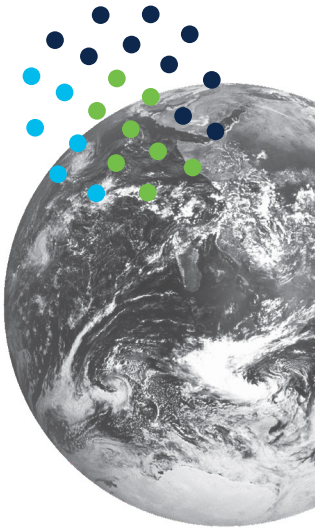
واقع جديد وأكثر تعقيدًا

على الرغم من أن هذه الابتكارات تسمح بوجود بيئة عمل أكثر ترابطًا وإنتاجية، إلا أنها قد غيرت تمامًا من طبيعة الطريقة التي نمارس بها الأعمال. لقد تحولت أيام التحكم في التطبيقات وتفويض المستخدمين محليًا في أماكن العمل إلى أنظمة اتصالات مشتركة ديناميكية متعددة السحابات تقدّم الخدمات والتطبيقات عبر المؤسسات. ليس ذلك فحسب، فنحن ندير أيضًا علاقات الأطراف الخارجية المهمة للأعمال. فالتوسع الضخم والاستعانة بمصادر خارجية يحققان سلوكيات اقتصادية في الحجم والكفاءة، ولكن لم يخلُ الأمر من المقايضات. فقد أدى هذا التطور في البنى الأساسية للشبكات إلى زيادة كبيرة في الأسطح المعرّضة للهجوم لدينا وجعل مهمة حماية شبكات الأعمال والبيانات والمستخدمين أكثر تعقيدًا بشكل صادم.

المكافحة من جديد باستخدام منتجات النقاط

لقد حاولت المؤسسات، كالمعتاد، معالجة هذه التحديات عن طريق إضافة حل الأمان "أفضل" نقطة لمعالجة كل مشكلة جديدة عند ظهورها. وبسبب هذا النهج، فقد رأينا "تمدّدًا" هائلًا للأجهزة، حيث استخدمت المؤسسة المتوسطة ما يصل إلى 75 نوعًا من أدوات الأمان[1]. ويمكن أن تؤدي منتجات الأمان المتعددة عبر مورّدين مختلفين إلى تعرّض فرق أمان الشبكة لمشاكل إدارية كبيرة. في معظم الحالات، يؤدي تكاثر أجهزة وإمكانات الأمان إلى زيادة في مخاطر الهجوم. فقد عبّر 94% من محترفي IT (تكنولوجيا المعلومات) و InfoSec (أمان المعلومات)، عند سؤالهم، عن شعورهم بالقلق من أن زيادة تعقيد الشبكة يزيد من تعرضهم للمخاطر، ويرغب 88% في جعل تغييرات سياسة أمان الشبكة أكثر مرونة[2].

في الفترة بين يناير و يوليو من عام 2019، تم الكشف عن 3800 حالة اختراق بيانات - بارتفاع نسبته 54% خلال النصف الأول من عام 2018[3]. ويعد هذا الصعود الحاد بمثابة شهادة على الأساليب المتطورة باستمرار التي تستخدمها الجهات الفاعلة السيئة لاختراق الشبكات. كما يعد المعدل المتنامي للاختراقات الناجحة إشارة إلى أن الطرق التقليدية لأمان الشبكة لم تعد تقف ضد التهديدات الحديثة.



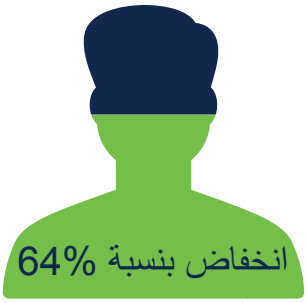
1 "Defense in depth: Stop spending, start consolidating" (الدفاع المتعمق: توقف عن الإنفاق، ابدأ الدمج)"، CSO، 4 مارس 2016.
2 "Navigating Network Security Complexity" (اجتياز تعقيد أمان الشبكة)"، تقرير ESG Research Insights، يونيو 2019.
3 "Navigating Network Security Complexity" (اجتياز تعقيد أمان الشبكة)"، تقرير ESG Research Insights، يونيو 2019.

مزيد من التهديدات، مزيد من التشويش، وأيضًا مزيد من المخاطر

في الوقت الذي تهاجم فيه الأطراف الخبيثة متجهات جديدة - بدءًا من البريد الإلكتروني مرورًا بنقاط النهاية غير المحمية بموجب سياسات BYOD، وصولاً إلى البوابات الإلكترونية وأجهزة إنترنت الأشياء، تُدفع المؤسسات أيضًا إلى تجربة أي عدد من النُهُج الأخرى لحماية نفسها.

وكما ذكر أعلاه، لا يؤدي اتجاه إضافة منتجات النقاط إلى تحسين وضع الأمان العام للمؤسسة. بل على العكس تمامًا. فهي تُحدث مزيدًا من "التشويش" لفرق الأمان لأجل إدارتها. فبينما تكافح هذه الفرق للتركيز على مراقبة الهجمات الجديدة التي لا مفر منها والبرامج الضارة التي تسعى إلى استغلال أي ثغرة أمنية (معروفة أو غير معروفة)، يجعل هذا التعقيد المضاف مهمة إنشاء سياسات أمنية وإدارتها وفرضها أمرًا أكثر صعوبة من أي وقت مضى.

واستجابةً لذلك، كُلِّفت فرق أمان الشبكة بتكوين تجمعات متعددة من الموارد السحابية كل على حدة، مما يزيد من فرصة حدوث تكوين أمني خاطئ قد يؤدي إلى حدوث اختراق. يمكن أن يكون أكبر متسبب في المشكلة على الإطلاق هو عنصر تحكم أمني لم يتم تنفيذه أو تم تنفيذه مع وجود أخطاء: 64% من المؤسسات تقول إن الخطأ البشري كان السبب الرئيسي للتكوين الخاطئ[4]. سواء كان مثل هذا الخطأ يؤدي إلى انتهاك للامتثال أو تعطّل أو فتح الباب أمام خصم، فإنه خطر لا يمكنك تحمله.



الخطأ البشري كان السبب الرئيسي وراء التكوين الخاطئ

حان الوقت لإعادة النظر في جدار الحماية.

أصبح أمان الشبكة مهمة شاقة. لا يستطيع الموظفون الحاليون المضي قدمًا في محاولة إدارة مجموعة متنوعة كبيرة من حلول أمان النقاط والموارد السحابية والأجهزة. لقد حان الوقت لاتباع نهج مختلف.

لقد حان الوقت لكي يحتل جدار الحماية موقعه كأساس لنظام أساسي لأمن الشبكة يتسّم بالمرونة والتكامل وهو ما سيقود شركات الأعمال في الحاضر والمستقبل.

القسم 2: من جدار الحماية إلى توزيع جدران الحماية

لماذا توزيع جدران الحماية؟

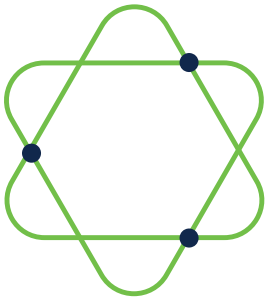
في ظل تطور شبكاتنا لتتواءم مع الطرق الجديدة لأداء الأعمال، يجب بالمثل أن يتطور أمان الشبكة لدينا. في عالم أصول تكنولوجيا المعلومات الموزعة الحالي، ما يزال جدار الحماية مركزيًا بالنسبة لوضع الأمان القوي.

ومع ذلك، فقد زادت متطلبات جدار الحماية بشكل كبير لحماية مجموعة كبيرة من البنى الأساسية للشبكة والأجهزة المتصلة وأنظمة التشغيل من التهديدات المتقدمة. وبالتالي، يتم تعزيز أجهزة جدار الحماية "التقليدية" لدينا من خلال مزيج من الأجهزة المادية والافتراضية - بعضها يتم تضمينه في الشبكة بينما يتم تقديم البعض الآخر كخدمة، أو تستند إلى مضيف، أو يتم تضمينها في البيئات السحابية العامة. حتى أن البعض يأخذ عوامل شكل وتصميم جديدة، مثل الأجهزة المجمّعة التي تتوافق مع متطلبات حركة مرور البيانات الضخمة والبرامج التي تعمل على الأجهزة الشخصية وموجهات SD-WAN وبوابات الإنترنت الآمنة. يعد نشاط مشاركة التحليل الذكي لمواجهة التهديدات عبر جميع أجهزة جدار الحماية المتباينة هذه، بغض النظر عن موقعها، أمرًا حيويًا لتحقيق الرؤية الموحدة للتهديدات ووضع أمان قوي.

لتحقيق التحول الكامل وتأمين الشبكات الحالية بدرجة أكبر، يجب على الشركات الابتعاد عن نهج "المحيط" التقليدي. وبدلاً من ذلك، فعليهم إنشاء نقاط التنفيذ الاستراتيجية عبر الموصلات البينية للشبكة بأكملها، بالقرب من المعلومات أو التطبيقات التي يتعين حمايتها. وعلى وجه التحديد، أصبح إنشاء طبقات محيطة صغيرة عند نقاط التحكم المادية والمنطقية على السواء واقعًا ضروريًا.

نحن بحاجة إلى التفكير بدرجة أقل في *جدار الحماية* كجهاز شبكة مادي مستقل وإلى مزيد من المعلومات حول توزيع جدران الحماية.

4 "Cloud Security Breaches and Human Errors (الاختراقات الأمنية للسحابة والأخطاء البشرية)"، Fugue، 7 فبراير 2019.



ما المقصود بتوزيع جدران الحماية؟

صدّقوني: جدار الحماية أكثر أهمية من أي وقت مضى. في الواقع، لتأمين شبكات اليوم نحتاج إلى **مزيد من** توزيع جدران الحماية **في كل مكان**. يتمثل الفرق في أن توزيع جدران الحماية يركز على **الكيفية** التي يمكنك بها إنشاء عناصر تحكم قائمة على السياسة في كل مكان:

يمكن لتوزيع جدران الحماية من الحماية أن يوفر نهجًا يتسّم بالمرونة والتكامل للسياسات المركزية ووظائف الأمان المتقدمة والتنفيذ المتسّق عبر شبكاتك غير المتجانسة متزايدة التعقيد. كما يجب أن يوفر طبقات حماية شاملة وإمكانية الرؤية وتناسق السياسات ومصادقة أقوى للمستخدمين والأجهزة. يجب أن يستفيد أيضًا توزيع جدران الحماية من مشاركة التحليل الذكي لمواجهة التهديدات عبر جميع نقاط التحكم لإنشاء إمكانية الرؤية الموحدة للتهديدات والتحكم فيها - مما يقلل بشكل كبير من الوقت والجهد المطلوبين لاكتشاف التهديدات وتقصّيها ومعالجتها.

وبهذه الطريقة، يصبح توزيع جدران الحماية استراتيجية أساسية لتأمين شبكتك المعقدة اليوم. كما أنها توفر جسرًا نحو المستقبل مع استمرار تطور أعمالك - ومشهد التهديدات.

كيف يبدو؟

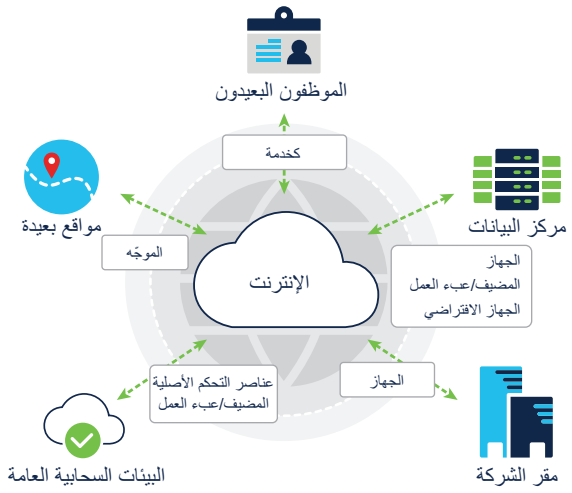
سواءً بغرض حماية الأصول والبيانات في السحابة أو محليًا في أماكن العمل أو في موقع بعيد، يحتاج توزيع جدران الحماية إلى توفير طبقات حماية متطورة ضد التهديدات وفرض السياسات والتحليل الذكي لمواجهة التهديدات المشتركة. ويتمثل التحدي في تقديم هذا الاتّساق عبر بيئات متباينة حيث يتم نشر أجهزة مختلفة واستخدامها.

يمكن أن تنشأ الاختراقات الأمنية من أي جهاز لديه إمكانية الوصول إلى الإنترنت، بغض النظر عما إذا كان في المقر الرئيسي للشركة أو في مركز البيانات أو في المواقع البعيدة أو السحابات العامة أو في أي موقع يعمل فيه أحد الموظفين عن بعد. وذلك هو السبب في زيادة أهمية تضمين مجموعة قوية من نقاط التحكم الأمنية في مواقع أكثر منطقية لتقليل التعرض وتخفيف المخاطر عن أي وقت مضى. يتم تطبيق عناصر التحكم في الأمان عند الحاجة إليها على البيئات المملوكة (الأجهزة المادية أو الافتراضية وأجهزة الشبكة مثل الموجّهات) فضلاً عن البيئات غير المملوكة (الأمان كخدمة [SECaaS]) وعناصر التحكم الأصلية وأعباء العمل.

ما المقصود بتوزيع جدران الحماية؟

تنتشر اليوم نقاط التنفيذ في كل مكان عبر الشبكات غير المتجانسة.

يقدم توزيع جدران الحماية وظائف متسّقة لمنع التهديدات مع سياسة وإمكانية رؤية متسّقتين للتهديدات بحيث يمكنك منع الهجمات واكتشافها وإيقافها بشكل أسرع ودقة أكبر في كل مكان.



الشكل 3. المستأجرون الأساسيون في توزيع جدران الحماية كوسيلة لمعالجة التحديات الأمنية للشبكات الحديثة

توسيع نطاق عناصر التحكم في الأمان

تحت فرضية وجود جدار الحماية التقليدي، ونظرًا لأن حركة مرور البيانات الداخلية بالكامل والمستخدمين المفوضين كانوا جديرين بالثقة بطبيعتهم (ولم تكن حركة مرور البيانات الخارجية كذلك)، فقد تم إنجاز مهمة حماية المؤسسة بأكملها على محيط الشبكة. وقد أصبح محيط الشبكة هذا هو نقطة التحكم الأمنية المنطقية لحماية المؤسسة بأكملها. تم توجيه حركة مرور بيانات الشبكة بأكملها، سواء الصادرة من المقر الرئيسي أو مركز بيانات أو عامل بعيد، من خلال نقطة التحكم الوحيدة هذه.

بالطبع، لا يعمل هذا النموذج في البيئات المعقدة الحالية التي تمتد فيها البنية الأساسية لتكنولوجيا المعلومات الخاصة بالمؤسسة في مجموعة متنوعة من عوامل الشكل والتصميم وطُرُز التسليم، بما في ذلك الأجهزة المادية والافتراضية أو الموجّهات أو المحولات المضمّنة في الشبكة، أيًا ما كانت مقدمة كخدمة أو مستندة إلى المضيف أو مضمّنة مع سحابة عامة.

ومن خلال أسلوب لتوزيع جدران الحماية، يتم نشر عناصر تحكم أمنية متسقة لتوفير إمكانية الرؤية الكاملة وفرض سياسة موحدة وإمكانية رؤية شاملة للتهديدات. تتيح عناصر التحكم في الأمان هذه مصادقة أقوى للمستخدمين والأجهزة عبر البيئات غير المتجانسة على نحو متزايد. حيث يمكنها تجميع السياق حول المستخدمين والمواقع والأجهزة، ومشاركتها والاستجابة لها، وغير ذلك الكثير لضمان تلبية الأجهزة لمتطلبات الأمان المحددة. باستخدام عناصر تحكم أمنية متسقة في كل طبقة محيطة صغيرة، يمكن لفرق الأمان البدء في أتمتة المهام (مثل العزل التلقائي للمستخدمين والأجهزة الخارجة عن الامتثال، وحظر المجالات المشكوك فيها عبر جميع عناصر التحكم في الأمان، ودعم التجزئة الدقيقة الفعالة). في توزيع جدران الحماية، توفر إمكانية الرؤية الكاملة نظرة شاملة لجميع تنبيهات الأمان ومؤشرات الاختراق، كما يوفر التحليل الذكي لمواجهة التهديدات المشتركة أحدث نهج للكشف عن التهديدات لأي جهاز متصل.

الإدارة المستندة إلى السحابة

وهي ليست مجرد منتجات نقاط فحسب. فقد أدت الزيادات الهائلة في الطبقات المحيطة للشبكة والموارد السحابية إلى زيادة التعرض للاختراقات أيضًا. لا تعدّ حماية أصول الشركة الأكثر قيمة في البيئات السحابية المعقدة مع إدارة منتجات الأمان المختلفة بالمهمة البسيطة. حيث تحتاج فرق الأمان إلى إمكانية رؤية فورية وإدارة مبسّطة للمساعدة في تقليل حالات التكوين الخاطئ.

يؤدي توزيع جدران الحماية إلى وضعية أمان أقوى من خلال دعم الإدارة المركزية والقائمة على السحابة لمساعدة فرق الأمان على التغلب على التعقيد ومواءمة السياسات في جميع أنحاء المؤسسة. يمكن للقوالب تحسين تصميم السياسات واتساقها عن طريق كتابة سياسة ما مرة واحدة وتوسيع نطاق فرضها عبر عشرات الآلاف من عناصر التحكم بالأمان عبر الشبكة. يؤدي استخدام قوالب السياسة القياسية لنشر أجهزة جديدة بسرعة إلى المساعدة في تقليل أخطاء التكوين. في ظل نمو المؤسسات، تزِث عمليات النشر الجديدة أحدث السياسات بشكل تلقائي. يعمل نظام إدارة السياسة القابل للتوسّع على دمج ميزات الأمان المتعددة في سياسة وصول واحد وتحسين السياسات على مستوى جميع أجهزة الأمان لتحديد التناقضات وتصحيحها بسرعة.

والأكثر من ذلك، أن حل الإدارة المركزي القائم على السحابة ينقل إمكانات الفريق إلى مستوى أعلى. فيمكنهم بالتالي التعرّف على المخاطر بسرعة عبر جميع الأجهزة، ما يجعلهم في حالة أكثر اتساقًا وأمانًا. باستخدام وحدة تحكم واحدة في الإدارة، يمكن مقارنة الكائنات عبر جميع الأجهزة للكشف عن التناقضات وتحسين وضع الأمان الحالي. يستطيع الموظفون تبسيط إدارة السياسة، وتحسين الكفاءة، وتحقيق أمان أكثر اتساقًا مع تقليل التعقيد في الوقت نفسه.

المعركة من جديد باستخدام التحليل الذكي لمواجهة التهديدات

مع التوسّع في محيط الشبكة وتكاثر عدد الأجهزة المتصلة مباشرة بالإنترنت، تتوسّع أسطح الهجوم لدينا كذلك. تهديدات الأمن السيبراني التي تنطوي على البرامج الضارة، والعملات المشفرة، والتصيد الاحتيالي، ونشاط روبوت الشبكة تتصاعد حدتها، ومحترفو الجرائم الإلكترونية يتحولون صوت تعلم الآلة والذكاء الاصطناعي لاستغلال الثغرات الأمنية الموجودة في البرامج وتسريع الهجمات الضارة. عدد قليل جدًا من المؤسسات تتوفر لديها موارد كافية لاختبار وتأهيل جميع تصحيحات الثغرات الأمنية الخاصة بمورِّدي البرامج - ويواجه معظمها تحديًا للتصدي لهجوم التهديدات الناشئة والمتطورة.

يمكن هنا لجانب آخر مقنع في توزيع جدران الحماية أن يقدم المساعدة. فالاستفادة من ذكاء التهديدات الرائدة في المجال من خلال أحدث أبحاث التهديدات - والتي أُجري بعضها على أحدث معلومات ممكنة - مع الوصول إلى تحديثات الحماية يساعدان على التخفيف من حدة تيار التهديدات المستمر. يحدد القائمون على أبحاث التهديدات مؤشرات الاختراق سريعًا ويتأكدون من وجود التهديدات ويشاركونها بسرعة. وباستخدام الادخارات الاقتصادية في الحجم، فإنهم يهدفون إلى حماية المؤسسات من التهديدات المتطورة قبل حدوثها. تعمل مشاركة التحليل الذكي لمواجهة التهديدات عبر الشبكات المتصلة فيما بينها وكذلك نقاط النهاية وأعباء العمل والبيئات السحابية على مساعدة فرق الأمان على ربط الأحداث التي تبدو غير متصلة بها والتخلص من التشويش وإيقاف التهديدات بشكل أسرع.

ما هي مخاطر عدم توزيع جدران الحماية؟

في ظل نقدم الشبكات، فإن المؤسسات قد قامت بالتكيف ونشر منتجات نقاط متنوعة لدعم متطلبات الأعمال والعمليات التجارية. وقد قاموا بالأمر نفسه عند الإعلان عن متجهات الهجوم الجديدة، بإضافة منتج تلو آخر للحماية من أحدث تهديد XYZ. وأولئك الذين يعتمدون على جدار حماية تقليدي لتأمين كل جهاز متصل عبر طبقات محيطة متعددة يعرضون بياناتهم وأصولهم الأكثر قيمة لمخاطر الاختراقات الأمنية. وفقًا لتقرير Cybersecurity Almanac لعام 2019، ستبلغ تكلفة أضرار الجرائم السيبرانية التي سيتكبدها العالم 6 تريليونات دولار أمريكي سنويًا بحلول عام 2021[5].

من الممكن أن تتسلل هذه التهديدات إلى الشبكة بسرعة وتهدد عمليات الشركة التي تفتقر إلى أمان الشبكة الشامل وإمكانية رؤية نقاط النهاية.

ومع ذلك، فإن تأمين شبكة مؤسسة ما وبيئاتها السحابية وأجهزتها وبياناتها أينما كانت يمثل عبئًا كبيرًا على فرق الأمان.

يبدأ توزيع جدران الحماية من جدار الحماية وينتهي عنده ليكون جدار الحماية بمثابة حجر الزاوية في حماية أمان الشبكة المستقبلي

في Cisco، عملنا بجد لتحقيق هذه الرؤية إلى واقع. ونحن نعمل مع شركات ومؤسسات من جميع الأحجام حول العالم، وجميعها بحاجة إلى تأمين شبكاتها لكي تكون أكثر مرونة وأكثر تكاملاً - وبتأمينها في قلب الشبكة نفسها. ولذلك السبب فإننا نوفر البنية التقنية الأكثر أمانًا على الإطلاق، وهي عبارة عن نظام أساسي قوي وشامل مع وجود جدار الحماية كأساس فيه.

ويُعد توفير مستوى غير مسبوق من الحماية من خلال هذا المفهوم أحد المكونات الرئيسية في استراتيجية الأمان لدينا. تمنحك محفظة أمان Cisco ومجموعة جدران الحماية من Cisco خطوة استباقية أمام التهديدات المتطورة باستخدام عناصر التحكم في الأمان ذات المستوى العالمي في كل مكان تحتاج إليها فيه وسياسة وإمكانية رؤية متسّقتين وابتكارات لتحسين العمليات الأمنية.

في عصر كان فيه مشهد التهديدات أكثر ديناميكية من ذي قبل، تجمع Cisco قيادة الشبكات والتكنولوجيا المتطورة معًا بحيث يمكنك الحصول على أقوى وضع أمان متوفر في الحاضر والمستقبل.

5 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics 2019" (100 حقيقة ورقم وتنبؤ واحصائية)"، Cybercrime Magazine، 6 فبراير 2019.

توفر جدران الحماية التقليدية نظرة محدودة؛ بينما تحتاج تكنولوجيا المعلومات إلى إمكانية رؤية أكبر عبر الشبكة بأكملها باستخدام التحليل الذكي لمواجهة التهديدات المشتركة لاكتشاف التهديدات وحظرها في وقت أسبق وأسرع. ويمتد توزيع جدران الحماية إلى أبعد من ذلك من خلال تقديم وضع أمان شامل يستند إلى إدارة موحدة وإمكانات أمان شاملة مثل منع الاقتحام وتصفية عناوين URL والحماية المتقدمة من البرامج الضارة التي تستفيد من الأتمتة وتعلم الآلة بحثًا عن الكفاءة.

بدون وضع استراتيجية لتوزيع جدران الحماية، يمكن أن يؤدي تعقيد الشبكة إلى تكوينات خاطئة، مما يؤدي إلى تصعيد الخطر إلى اختراق أمني. وفقًا لتقرير Gartner، "حتى عام 2022، ستكون هناك نسبة لا تقل عن 95% من إخفاقات الأمان السحابي بسبب خطأ العميل."[6] من خلال تبني استراتيجية لتأسيس نهج لجدار الحماية لتنسيق سياسات الأمان عبر نقاط التحكم المتعددة، تعمل المؤسسات على تحسين وضع الأمان العام لديها.

القسم 3: الخطوات الأربع لإعداد استراتيجيتك الخاصة بتوزيع جدران الحماية

الخطوة 1: ضع الأساس لاستراتيجيتك الناجحة لتوزيع جدران الحماية باستخدام جدار حماية حديث من الجيل التالي. سيقدم جدار الحماية الآمن من Cisco المناسب سياسات أمان متسقة وإمكانية الرؤية والاستجابة المحسّنة للتهديدات لحل الأمان المتكامل لديك.

الخطوة 2: بمجرد اختيارك لجدار الحماية الآمن من Cisco الخاص بك، ستكون الخطوة التالية هي المعايرة على أحد حلول الإدارة. ضع في الاعتبار هذه العوامل عند تحديد الحل المناسب لمؤسستك:

- تحديد موقع الإدارة المفضلة (محليًا في موقع العمل، أو على السحابة) والمجموعة التي ستكون مسؤولة عن إدارة الأمان (SecOps أو NetOps).
- والأهم من ذلك كله، ضمان توافق حل الإدارة مع الأهداف الحالية والمستقبلية لتكنولوجيا المعلومات. إذا كنت تنقل أعباء العمل إلى السحابة، أو تطلق بوابة مورّد، أو تتعامل مع مشاريع التحول الرقمي أو تطبيقات SaaS، فقد تحتاج إلى تبني حل إدارة قائم على السحابة. إذا كانت مؤسستك تعتمد على التطبيقات القديمة المتجانسة، فقد تتناسب التطبيقات المحلية في موقع العمل مع احتياجاتك. وبوجه عام، تحتاج التطبيقات القديمة إلى إعادة تكوينها نوعًا ما لتعمل بشكل صحيح على السحابة، وإذا لم تكن هناك خطط فورية لترقية هذه التطبيقات، فمن الأفضل عادةً وجود نظام إدارة محلي في موقع العمل.
- يساعد حل الإدارة القائم على السحابة فرق عمليات الشبكة في تنظيم السياسات على مستوى المؤسسة وتقليل التعقيد وإدارة جميع نقاط التحكم في الأمان من لوحة معلومات مركزية. كما يعمل على تبسيط سياسات التنسيق والإدارة باستمرار من مكان واحد وذلك للحماية من أحدث التهديدات. من خلال تطبيق مركزي قائم على السحابة، يمكنك تبسيط إدارة الأمان ونشر الأجهزة الجديدة بشكل أسرع باستخدام القوالب وتتبع جميع التغييرات بمرور الوقت على مستوى بيئتك.

الخطوة 3: تقوية وضع الأمان لديك من خلال التكامل. يجب أن توفر استراتيجيتك لتوزيع جدران الحماية تغطية شاملة على مستوى جميع الطبقات المحيطة الدقيقة وتقدم الحماية والتحكم على مستوى جميع الأجهزة المتصلة وحلول الأمان. يعمل دمج الأمان في جميع أجزاء شبكتك غير المتجانسة وعبر تطبيقات وخدمات السحابة والبريد الإلكتروني للشركة وجميع نقاط النهاية المتصلة على حماية شركتك من مشهد التهديدات المتزايدة.

تؤدي هذه الخطوة إلى إعداد فريق الأمان لديك لحظر المزيد من التهديدات والاستجابة بشكل أسرع للتهديدات المتقدمة وتقديم الأتمتة عبر الشبكة إلى التطبيقات السحابية ونقاط النهاية.

الخطوة 4: وأخيرًا، تأكد من تضمين استراتيجيتك لتوزيع جدران الحماية لتحليل التهديدات المتقدمة المستمرة وذلك لحماية أصول شركتك ومساعدتك في أن تبقى على اطلاع بالتهديدات الناشئة الجديدة. وتتمثل إحدى أسهل الطرق لتحقيق ذلك في اختيار حل يوفر تلقائيًا أحدث معلومات التهديدات لشبكتك من خلال جدار الحماية لديك. يتيح كل من التحليل الذكي المحدّث وإمكانية الرؤية الكاملة لفرق الأمان إمكانية فهم أحدث الثغرات الأمنية. وإذا كان التهديد قد شق طريقه في الاختراق، فيمكنك تحديد مكانه وكيفية حدوثه. تعمل وظائف IPS المدمجة من الجيل التالي على أتمتة تصنيفات المخاطر وإشارات التأثير لتحديد الأولويات بحيث يمكن التعرف على الأصول والمعلومات الأكثر أهمية وتحديد أولوياتها. يمكن لفرق الأمن على الفور اتخاذ إجراء تصحيحي ومعالجة التهديدات، للحفاظ على التركيز على الأصول الأكثر أهمية مقابل أن يطغى عليها "التشويش"، مما يجعل عمليات SOC (مركز العمليات الأمنية) أكثر أمانًا.

6 "Is the Cloud Secure?" (هل السحابة آمنة؟)" Gartner، 27 مارس 2018.

الأمر يبدأ بجدار الحماية المناسب كأساس

تحتاج فرق الأمن اليوم إلى ما يلي:

أمان أفضل يدعمه التحليل الذكي لمواجهة التهديدات الرائد في المجال لحماية شبكتك المعقدة واكتشاف التهديدات في وقت أسبق والعمل بشكل أسرع.

طريقة لأجل **تعيين سياسات الأمان وتوسيع نطاقها وتنسيقها** على مستوى شبكتك.

إمكانية الرؤية وتقليل التعقيد مع الإدارة الموحدة والأتمتة لتسريع العمليات الأمنية وتحسين تجاربها.

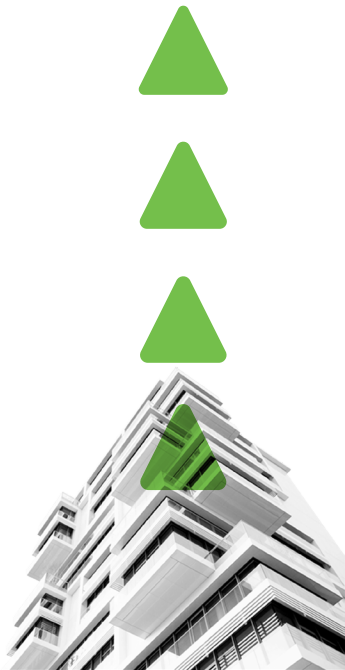
شبكات وأمان يعملان معًا لزيادة استثماراتك الحالية لأقصى حد. وسيعمل الحل المناسب على توفير مجموعة كبيرة من التكاملات للأمان الشامل تحمي كل شيء، في كل مكان.

مزايا استراتيجية توزيع جدران الحماية مع جدار الحماية الآمن Cisco Secure Firewall

حوّل شبكتك بأكملها إلى امتداد لبنية الأمان التقنية لديك: من خلال مشاركة السياسة المشتركة وإمكانات منع الاقتحام وغيرها من الوظائف الأساسية مع جدار الحماية الآمن Cisco Secure Firewall، يمكن للمحولات والموجهات أداء عمليات فرض الأمان، وذلك بربط البنية التحتية للشبكة في محفظة أمان شاملة. يمكنك مشاركة التحليل الذكي لمواجهة التهديدات عبر البنية التقنية بسرعة لربط الأحداث غير المتصلة في ظاهرها والقضاء على التشويش وإيقاف التهديدات على نحو أسرع.

عناصر تحكم أمنية عالمية المستوى: يوفر جدار الحماية الآمن Cisco Secure Firewall فعالية فائقة في مواجهة التهديدات لحماية شبكتك المعقدة من الهجمات الحالية المتطورة بشكل متزايد. يساعد التحليل الذكي لمواجهة التهديدات المتقدمة الرائدة في المجال مؤسستك في العثور على نطاقات جديدة من البرامج الضارة وعناوين URL الضارة بالإضافة إلى الثغرات الأمنية غير المعروفة أو غير المعلنة للكشف عن التهديدات في وقت أسبق وللعمل على نحو أسرع. يقدم نظام كشف الاقتحام (IPS) المضمن من الجيل التالي إمكانية رؤية شاملة بتصنيفات مخاطر تلقائية وإشارات تأثير لتحديد الأولويات لفريق الأمن، مما يقلل من التشويش لأدنى حد. يبقيك الأمان الارتجاعي على علم بآخر المستجدات ويحلل التهديدات باستمرار بعد الكشف الأولي وذلك لتحسين التعرف على البرامج الضارة المتطورة التي قد تكون مخفية في البداية.

رؤية موحدة للسياسة وإمكانية رؤية التهديدات: يمكن لفرق الأمان تحقيق اتساق السياسات وتناسقها من خلال توحيد معايير عناصر التحكم في الأمان ودفعها عبر كل جهاز - بدءًا من أجهزة الشبكة وصولاً إلى الأجهزة المضيفة وعبر السحابة. تتيح إدارة Cisco المرنة والمركزية لفريقك تطبيق عناصر تحكم قابلة للتوسع على العديد من الأجهزة بسرعة وسهولة للحفاظ على السياسات المتسقة. يمكنك التقليل من التعقيد من خلال الإدارة الموحدة والربط المؤتمت للتهديدات عبر وظائف الأمان المتكاملة بإحكام، بما في ذلك توزيع جدران الحماية للتطبيقات و NGIPS (نظام كشف الاقتحام من الجيل التالي) و AMP (الحماية من البرامج الضارة المتقدمة). يمكنك تبسيط سياسة الأمان وإدارة الأجهزة عبر الشبكات الممتدة وتسريع عمليات الأمان الأساسية مثل الاكتشاف والتفصي والمعالجة.



القسم 4: حل أمان جاهز للمستقبل

لقد تغيرت الطريقة التي نعمل بها. لقد قامت أعمالنا وشبكاتنا بتحويل قواعد أمان الشبكة وتغييرها. تتطلب منا هذه التطورات إعادة التفكير في جدار الحماية وتبني توزيع جدران الحماية.

تدفع Cisco بالابتكارات للتعامل مع هذه الاتجاهات من خلال نظام أمان أساسي يوفر عناصر تحكم في أمان على مستوى عالمي في كل مكان تحتاج إليها فيه من خلال سياسات أمان متسّقة وإمكانية الرؤية، مدعومة بالتحليل الذكي لمواجهة التهديدات الرائد في المجال. يُعد الجيل الأخير من جدار الحماية الآمن Cisco Secure Firewall أساس محفظتنا من المنتجات المتكاملة تمامًا.

يوفر حل إدارة السحابة الرائد من Cisco - **Cisco Defense Orchestrator** - تناسق السياسة عبر مجموعة متنوعة من منتجات الأمان من Cisco.

مرفق في كل منتج أمان من Cisco **الاستجابة الآمنة للتهديدات**، وهو حل يتم تشغيله تلقائيًا للاستجابة للتهديدات يتفاعل مع الهجمات الإلكترونية الجديدة من خلال مشاركة ونشر التدابير المضادة تلقائيًا عبر بنية الأمان التقنية بأكملها.

Secure Endpoint (نقطة النهاية الآمنة) تقدم التحليل الذكي لمواجهة التهديدات العالمية، وآلية وضع الحماية المتقدمة، وحظر البرامج الضارة في الوقت الحقيقي. تحلل AMP (حزمة الحماية المتقدمة من البرامج الضارة) أيضًا نشاط الملف باستمرار عبر الشبكة الموسعة لديك لأجل اكتشاف البرامج الضارة المتقدمة ومنعها من الانتشار وإزالتها بسرعة.

Talos Threat Intelligence هو فريق معروف على مستوى العالم يتكون من مجموعة من الباحثين في مجال التهديدات وعلماء البيانات والمهندسين الذين يجمعون معلومات حول التهديدات القائمة والمتطورة. يدعم Talos نظام الأمان البيئي في Cisco بالكامل ويوفر الحماية ضد الهجمات والبرامج الضارة. ويوفر Talos إمكانية رؤية لأحدث التهديدات العالمية، والتحليل الذكي القابل للتنفيذ بشأن الدفاع وتخفيف الحدة، والاستجابة الجماعية لتوفير الحماية الفعالة لجميع عملاء Cisco.

نظام منع الاقتحام من الجيل التالي من SNORT (SNORT NGIPS) هو نظام منع اقتحام من الجيل التالي (NGIPS) مفتوح المصدر ورائد في المجال يعمل على تحليل حركة مرور البيانات، ومراقبة/تسجيل الحزم، وتحليل البروتوكول. ويستفيد نظام SNORT NGIPS من التحليل الذكي من Talos لمواجهة التهديدات لمساعدة مجتمع الأمان بأكمله من خلال مشاركة السياسات التي توفر الحماية من التهديدات المتطورة.

يتوفر الوصول الموثوق والقابل للتكيف في كل مكان القائم على السياق مع محرك خدمات الهوية (ISE). كما أنه يوفر حماية ذكية ومتكاملة من خلال حلول الامتثال والسياسة القائمة على الغرض.

الوصول الآمن من خلال المصادقة ثنائية العوامل يوفر المصادقة متعددة العوامل وإمكانية رؤية نقاط النهاية والمصادقة التكيفية وفرض السياسة مع الوصول عن بعد وتسجيل الدخول الفردي للوصول الآمن إلى التطبيقات بشكل استباقي.

تحليلات الشبكة الآمنة، وعبء العمل الآمن، والبنية الأساسية المرتكزة على التطبيقات (ACI) تعمل معًا، وتستمر في مراقبة المستخدمين لديك أينما كانوا وأعباء العمل الخاصة بتطبيقاتهم في أي مكان يتواجدون فيه، وذلك باستخدام تعلم الآلة والنمذجة السلوكية وقياس بيانات البنية الأساسية للشبكة والتجزئة للتغلب على التهديدات الناشئة.

يمكنك تنفيذ استراتيجيتك لتوزيع جدران الحماية الجاهزة للمستقبل من خلال الاستثمار في نظام الأمان الأساسي من Cisco وفي جدار الحماية الآمن Cisco Secure Firewall. وستكتسب أقوى وضع أمني متوفر اليوم وستكون مستعدًا للغد.

القسم 5: ابدأ اليوم في بناء مستقبل جدار الحماية لديك

تجمع Cisco بين الريادة في مجال الشبكات وتكنولوجيا الأمان المتطورة معًا لتوفير البنية التقنية الأكثر أمانًا على الإطلاق. سواء أكنت تعمل على تعزيز أمان شبكتك من خلال تحسين الاستثمارات القائمة لأفضل ما يمكن أو تحويل الموجّهات لديك إلى جدار حماية، تواصل Cisco الابتكار.

جدار الحماية الآمن Cisco Secure Firewall هو أمان الشبكة المصمم لأعمالك ذات التحول الرقمي - من ذات الشركة التي قامت ببناء الشبكة.

تعرف على مزيد من المعلومات حول جدار الحماية الآمن **Cisco Secure Firewall** وابدأ اليوم مستقبل توزيع جدران الحماية لديك. واطلع على مزيد من المعلومات حول أحدث الاتجاهات في تشكيل شبكات المستقبل في **تقرير اتجاهات الشبكات العالمية لعام 2020**.