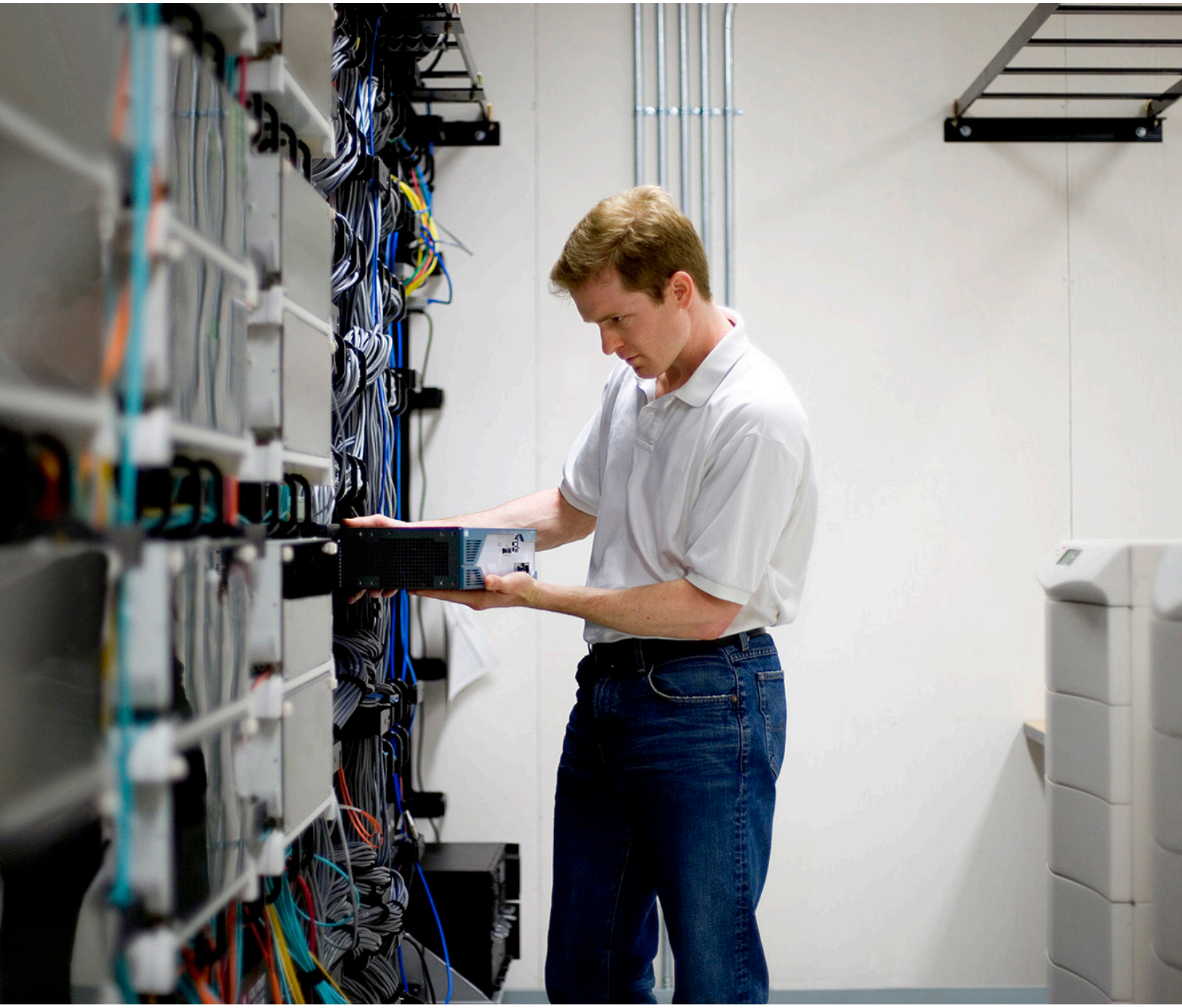
اجعل حافة شبكتك ذكية وتمكّن من تلبية الاحتياجات المستقبلية



الملخص التنفيذي

في ما يتعلق بحقيقة الأعمال الرقمية الجديدة، لم تكن حافة الشبكة أكثر أهمية من قبل مطلقًا. وبالرغم من أنه عادةً ما يتم إغفالها، فإن حافة الشبكة هي حجر الزاوية الذي إما أن يتم تحقيق النجاح الرقمي به أو خسارته. بالنظر إلى كل ما يحدث عند حافة الشبكة، تجد:

- إنها خط الدفاع الأول ضد تسلل الأجهزة غير الموثوقة أو الضارة.
- إنها القناة —المستغَلة بدرجة كبيرة غالبًا—المسؤولة عن توصيل تطبيقات وخدمات إلى الجمهور المستهدف.
- إنها البوابة الإستراتيجية للربط بين المؤسسات المنتشرة على نطاق واسع.
- إنها الجسر الرابط بين مؤسستك وعملائك.
- إنها بمثابة نقطة توصيل أجهزة إنترنت الأشياء (IoT) الجديدة وإدارتها.
- إنها الموضع الأمثل لفهم ما يحدث في عملك فعليًا.

يتم نشر حافة الشبكة أحيانًا مع الاعتقاد بأن جميع حلول الشبكات واحدة بشكل أساسي. تختلف Cisco مع هذا الرأي وتفسّر ذلك بأن الأعمال الرقمية الجديدة تستلزم نطاقًا واسعًا من الذكاء عند الحافة.

لذا نقدم الحلول والوظائف الإستراتيجية اللازمة لتحقيق نجاح الأعمال. تقوم Cisco بتشغيل حافة الشبكة الرقمية الجديدة بالتركيز على:

- الدفاع عن الأصول المهمة عند الحافة. يمكن للمؤسسات تفادي 99.2% من اختراقات الشبكات من خلال تعزيز الشبكة كجهاز استشعار وتعزيز. قد تقل هذه النسبة في حالة تقديم رؤى أكثر عمقًا لتحسين مستوى الوقاية وزيادة سرعة الاستجابة.
- تمكين الوعي بالتطبيقات والأجهزة مع زيادة سرعة التجوال بمعدل ثماني مرات أسرع ورؤية ما يزيد عن ١٢٠٠ تطبيق. ويكون ذلك ممكنًا من خلال شراكة إستراتيجية مع Apple وابتكارات تقنية Wi-Fi.
- التكيف السريع مع الشبكة نظرًا لأن عملك يتطور وفقًا لمنهج يتم تحديده بواسطة البرنامج على الشبكات LAN اللاسلكية وLAN وWAN. يؤدي هذا إلى انخفاض تكاليف النشر بنسبة 79% عن طريق فصل الأجهزة عن البرامج وجعل حافة WAN افتراضية.
- لذا يتعين إيجاد نظام أساسي مصمم لتلبية الاحتياجات المستقبلية عن طريق وضع أسس قابلة للبرمجة وقائمة على المعايير يمكنها إضافة وظائف جديدة بسرعة عند الحاجة إليها.
- تقديم رؤى أعمق وأسرع بشأن البيع بالتجزئة والفندقة والحصول على ما يصل إلى مقياس واحد بشأن تفضيل بيانات الموقع لاتخاذ قرارات أعمال أفضل.

تعد الشبكة في الوقت الحالي عنصرًا جوهريًا لتحقيق تغيير في جميع المؤسسات ظاهريًا أثناء سلوكها مسار التحول الرقمي. ستساعد رحلة التحويل هذه المؤسسات في زيادة السرعة وتحسين الإنتاجية والتواصل مع العملاء بشكل أفضل وحماية الأصول والممتلكات الفكرية الأساسية.

تلعب حافة الشبكة دورًا حيويًا في عملية التحويل هذه وقد يقع على عاتقها القدر الأكبر من المسؤوليات مقارنةً بالمركز وشبكات مراكز البيانات. كما هو موضح في الشكل ١، عند مقارنة كل طبقة من طبقات الشبكة، تتحمل حافة الشبكة نطاقًا واسعًا من المسؤولية بالمبنى. يعد هذا صحيحًا في هذا الفرع أيضًا.

الشكل ١. طبقات الشبكة ووظائفها

دور حافة الشبكة

يزيد التحول الرقمي من أهمية حافة الشبكة عما مضى. بالنظر إلى كل ما يحدث عند حافة الشبكة:

- **إنها خط الدفاع الأول.** فالحافة هي موقع تطبيق السياسة واختبارها، بدون تقييد قدرتك على الوصول إلى الأشياء التي تحتاج. في حالة عدم إدارة الوصول بشكل صحيح، فقد تصبح أعمالك عرضة لانتشار المخاطر أو التسلل إلى الشبكة وزيادة أحجام المخاطر التي تهدد الأعمال بقدرٍ ملحوظ. إذ يعد كلٌ من الجهاز والبرنامج الثابت، بل ونظام التشغيل أيضًا، نقاط اختراق.
- **إنها القناة التي تقدم تطبيقات مستثمَرة بشكل فائق.** فحافة الشبكة هي موقع تحديد الأولويات. ويؤدي سوء التشغيل عند الحافة إلى اقتناء تطبيق بطيء؛ الأمر الذي يؤدي بدوره إلى انخفاض عائد الاستثمار.
- **إنها بوابة إستراتيجية للربط بين المؤسسات المنتشرة على نطاق واسع.** يعد تقديم تجربة سلسة للموظفين والشركاء والعملاء—حيثما كانوا—مهمًا للغاية. ستقدم شبكة من الفئة الثانية مستويات متباينة من الخدمات إلى الجمهور الأساسي.
- **إنها الجسر الرابط بين المؤسسة وعملائها.** إذا كنت جزءًا من المؤسسات العاملة في مجال البيع بالتجزئة أو الفندقة، فسيقلل الوصول إلى الأجزاء الفرعية من قدرتك على التواصل مع العملاء على مستوى شخصي والتأثير سلبًا على علامتك التجارية.
- **إذ تم بناؤها لتقوية ودعم متطلبات أجهزة إنترنت الأشياء المتزايدة.** تتكيف حافة الشبكة مع البيئة الفعلية عن طريق نقل جميع المجالات ظاهريًا إلى العصر الرقمي عن طريق تطوير عمليات التشغيل وخفض التكاليف. وبدون العمل بالشكل الصحيح عند الحافة، قد تغفل المؤسسات فيما يتعلق بخفض التكاليف والكفاءات التشغيلية.
- **إنها الموضع الأمثل لفهم ما يحدث فيما يتعلق بالأعمال.** ففي أي شبكة موزعة، يمكن للحافة وحدها رؤية جميع حركات مرور البيانات، من خلال جمع البيانات والتحليلات من الحافة. يمكن للبيانات المتعلقة بالمستخدمين والتطبيقات والأجهزة والتهديدات أن تمهد للوصول إلى رؤى تساعد فعليًا في اتخاذ قرارات أفضل لدعم الموظفين، وتقليل المخاطر والتكاليف وتوصل معلومات إلى الجمهور المستهدف. وبدون تحقيق المستوى المناسب من التحبيب الدائم للشبكة، فقد يؤدي ذلك إلى انحراف البيانات وفقدان الثقة بها.

هل يعد تسليع حافة الشبكة أمرًا جيدًا؟

تهدف العديد من حلول الحافة إلى التسليع عن طريق الاعتماد على المكونات المتوفرة بالفعل لبناء أجهزة حافة الشبكة والتصميم المباشر وفقًا لمعايير المجال. وعادةً ما يتم ذلك بهدف تقليل تكاليف التصميم الهندسي وإنتاج الأجهزة عن طريق تعزيز التصميمات المتوفرة بالفعل المقدمة من قِبَل جهات تصنيع المكونات. ويؤدي ذلك إلى تسليع الحافة. إن منح منهج تقليل التكاليف والإدارة أولوية على تقديم ابتكارات متميزة في مجال الأمان والنمو يعرض أعمالك لخطر أكبر.

ما المقصود بالخطر؟

تتوفر المكونات والتصميمات ليس فقط لجهات تصنيع الأجهزة فحسب وإنما أيضًا يمكن أن تجد سبيلها للوصول إلى أيدي الأشخاص الذين يسعون للتسلل إلى الشبكة. يعد كل جهاز يتصل بالشبكة نقطة يمكن التسلل إلى الشبكة من خلاله. تعتمد المؤسسات في الوقت الحالي على عدد متزايد من الأجهزة المتنقلة وأجهزة إنترنت الأشياء (IoT) على شبكاتها لتحقيق النجاح في أعمالها. تحتاج المؤسسات الى البحث عن حلول تتعامل مع مسألة تأمين الوصول، ابتداءً من الحافة وصولاً إلى فحص وإعادة فحص حركة مرور البيانات عند كل خطوة ابتداءً من الحافة وصولاً إلى مركز البيانات.

كما أن هناك خطر الاضطرار إلى إعادة التصميم الهندسي للشبكة في حالة ظهور احتياجات أعمال جديدة. يتم تصميم حلول جاهزة لتلبية احتياجات عدد كبير من حالات الاستخدام الحالية، ولكنها محدودة من حيث المرونة وملاءمة طلب العميل. كما أنها محدودة من حيث استعدادها لمواجهة التطور غير المتوقع في مجال الشبكات لديك. يجب أن يتكيف نظام الشبكات مع متطلبات العالم الرقمي الحالي سريع التطور.

ويتم تصميم معظم الحلول الجاهزة من أجل الامتثال للمعايير المعمول بها في المجال تمامًا، تلك المعايير المهمة لتحقيق مجموعة أساسية من المتطلبات والوظائف. بالرغم من ذلك، فقد تتغير المعايير. تتسم عملية وضع المعايير بأنها عملية تمتد لفترات طويلة، في حين يتسم معدل إنتاج جهات تصنيع الأجهزة ومطوري التطبيقات ومتطلبات المستخدم بالتغيير المتواصل. لذا فقد تجد جهات التصنيع التي تتبع أسلوبًا قائمًا على المعايير أنفسها متأخرة في ما يتعلق بتلبية توقعات أعلى من قِبَل المستخدم. في بعض الأحيان يمكن أن يبدأ الحل وفقًا للمعايير، ولكن بعد ذلك يكون قادرًا على التطور بإضافة وظائف جديدة إلى تلك المعايير عند الحاجة. تلبي تلك الحلول المتطلبات الجديدة المطلوبة في العالم الرقمي دون الالتزام بالمعايير، التي قد تحتاج لسنوات طويلة لتطويرها وتعديلها.

هناك خطر آخر وهو الإضرار بتكامل الجهاز. تعترض بعض المؤسسات الخبيثة سبيل الأجهزة عند شحنها عالميًا، ثم تقوم بتغيير المكونات، مثل تبديل المعالجات أو دمج شاشات للحصول على بيانات حساسة.

ما التكلفة الفعلية؟

غالبًا ما يتم تسليع الحافة لتقليل تكاليف الهندسة والإنتاج، وإتاحة بيع بعض الحلول بأسعار أقل. ومع ذلك، عند تقييم التكلفة يجب عدم النظر إلى رأس المال الصافي فقط أو حتى تكاليف التشغيل، وإنما يجب علينا أيضًا النظر إلى التكاليف المصاحبة للخطر. تختلف كل مؤسسة عن غيرها، ومن ثَم لا يمكن تحديد التكاليف الفعلية التي تمثل جميع المؤسسات. ولكن يجب مراعاة:

- تكلفة الثغرة الأمنية. تعد الأصول والممتلكات الفكرية مصدر كسب العيش الرئيسي لدى العديد من المؤسسات. وإذا وقعت تلك الممتلكات في أيدٍ غير أمينة، فماذا ستكون التداعيات؟ تجيد المؤسسات الخبيثة جني الأموال من استغلال الممتلكات الفكرية بطريقة غير معقولة عن طريق طلب الفدية والابتزاز وإعادة بيعها لصاحب أعلى سعر. إذ كشفت بعض الدراسات أنه يتم افتداء السجلات الطبية مقابل ٤٠ دولارًا أمريكيًا لكل سجل. ومع وجود آلاف السجلات، قد تكون المستشفيات فريسة محتملة عن طريق ابتزازها وإجبارها على دفع الكثير من المال لاسترداد ممتلكاتها.
- تكلفة عدم تكيف الموظفين مع التطبيقات المهمة للأعمال. هناك العديد من المؤسسات التي تستثمر جزءًا كبيرًا من ميزانيتها في اقتناء تطبيقات وأنظمة جديدة لتحسين الإنتاجية. وإذا لم يُجِد الموظفون التعامل مع تلك التطبيقات والخدمات، فسوف يتجنبون التعامل معها ولن يتحقق عائد الاستثمار المرجو من اقتنائها.
- تكلفة الفرص الضائعة. إذا كنت تعمل بمؤسسة في مجال البيع بالتجزئة أو الفندقة، فأنت تتعامل مع العملاء عبر أجهزتهم المحمولة. ولكن إذا واجه عملاؤك صعوبات في التواصل، فهذا يعني خسارة مؤسستك فرصة التواصل مع هذا العميل والتأثير على السلوك المرغوب لديه.
- تكلفة عدم وضوح الرؤية. تزخر حافة الشبكة بكم كبير من المعلومات المتعلقة بالمستخدمين والأجهزة والتطبيقات التي يستخدمونها والأماكن التي يذهبون إليها وأيضًا معلومات حول أماكن المخاطر المحتملة. وفي ظل غياب هذه الرؤية، قد تهدر مؤسستك ساعات لا تُعد ولا تحصى في محاولة فهم كيفية تفاعل المستخدمين مع البيئة ووصولهم إلى المعلومات واستغلالها، حتى أنها قد تعجز عن اكتشاف الخطر المحتمل الذي كان من الممكن التصدي له مبكرًا.

تقدم شركة Cisco حلولاً ذكية عند حافة الشبكة

تتبع Cisco منهجًا مختلفًا عن تسليع الحافة. فنحن نستثمر بقوة في مجال تطوير ابتكارات يتم توظيفها للمساعدة في نقل المؤسسات الى العصر الرقمي. ونضع نُصب أعيننا الدفاع عن الأصول المهمة، وذلك لدعم مستوى أعلى من الوعي بالأجهزة والتطبيقات وتقديم رؤى أعمق وأسرع. تساعدك Cisco في التكيف مع تطور أعمالك والاستعداد لأي جديد يخفيه المستقبل لك. ونقوم بذلك عن طريق إنشاء وظائف فريدة من البداية أو تطوير الوظائف الموجودة في المكونات التي تم اختبارها بالفعل داخل موقع العمل. كما توفر Cisco الوظائف للمساعدة في تلبية احتياجات حافة الشبكة في الوقت الحالي وفي المستقبل.

الدفاع عن الأصول المهمة عند الحافة

حافة الشبكة هي النقطة الأولى للوصول غير المخول أو العدائي نظرًا لأنها نقطة تواجد المستخدمين والأجهزة على الشبكة. لذا يجب أن يتم الوثوق بها لتحديد ما يدخل على الشبكة والتحكم فيه.

إن الموافقة على أن تسليع أمان الحافة ستكون فعالة مما يدل على أن حلول الأمان الجاهزة ناجحة. ولكن إذا كان هذا صحيحًا، فما سبب زيادة حجم التعاملات في مجال سرقة المعلومات والابتزاز والفدية بسرعة حتى بلغت قيمتها تريليون دولار أمريكي؟

إن أساليب أمان الحافة الحالية لا تعمل. تحتل Cisco الريادة في ما يتعلق بابتكار التقنيات لمعرفة ماهية الشيء وطبيعته، فضلاً عن تحديد مدى جودته قبل إطلاقه على الشبكة والسماح له بالانتشار.

وفيما يلي عدد من الابتكارات المتعلقة بأمان حافة الشبكة من Cisco® من أجل عملاء Cisco وطريقة استخدامها:

- **هوية المستخدم والجهاز وسلامتهما**. تتضمن أجهزة الحافة من Cisco أكثر تقنيات فحص ملفات تعريف النقاط الطرفية شمولاً. بالإضافة إلى ذلك، يُجري عامل الأمان Cisco AnyConnect® فحص أمان للامتثال للسياسة والوضع قبل السماح بالوصول إلى شبكة الإنتاج. يعمل أكثر وسائل فحص الهوية عند النقاط الطرفية دقةً على إبعاد الأجهزة غير المخولة وغير الآمنة (المصابة بالبرامج الضارة) من الدخول إلى الشبكة تمامًا حتى يثبت خلوها من أي ضرر والحصول على تخويل.
- **امتيازات الوصول التي تتغير حسب درجة الخطر**. في ظل دمج محرك خدمات الهوية Identity Services Engine من Cisco، يمكن للمستخدمين والأجهزة الوصول إلى امتيازاتهم التي تتغير تلقائيًا عند تغير درجة احتمال تعرضهم لخطر STIX أو الثغرات الأمنية في CVSS. تعد STIX وCVSS تعبيرات شائعة الاستخدام لوصف مدى خطورة تهديدات الأمان والثغرات الأمنية.
- **دمج التجزئة المحددة بواسطة البرامج**. عادةً ما تكون تجزئة شبكات LAN وإدارتها باستخدام شبكات LAN ظاهرية وقوائم التحكم في الوصول (ACL) صعبة وتزداد صعوبتها كلما أصبحت التجزئة ضرورية لتأمين عمليات تشغيل إنترنت الأشياء. يتم شحن أجهزة الحافة من Cisco متضمنةً التجزئة المحددة بواسطة الجهاز Cisco TrustSec® ضمن نظام التشغيل فضلاً عن ASIC لضمان سهولة وجودة أداء تحديد الهوية والتجزئة من نقطة الوصول إلى التطبيق الموجود في مركز البيانات.
- **الشبكة كأداة تعزيز**. يعد هذا جزءًا مضمنًا محددًا من قِبَل البرنامج ضمن أجهزة الحافة، من شأنه السماح الفوري والدائم بتعزيز سياسة الأمان للتحكم في الوصول واحتواء التهديدات. قد يؤدي العمل من خلال التكامل مع محرك خدمات تحديد الهوية وCisco Stealthwatch والتقنيات المصاحبة لتقنية الأمان من Cisco إلى الحث على وضع سياسة جديدة للسيطرة على الخطر، وكل هذا عبر لوح زجاجي واحد - أو منتج واحد
- **الشبكة كأداة استشعار**. احصل على رؤية متقدمة من طرف إلى طرف مع NetFlow وترجمة من خلال Cisco Stealthwatch. ونظرًا لتضمين Flexible NetFlow في جميع أجهزة الحافة من Cisco، فيمكنك الاستمتاع برؤية تدفق من طرف إلى طرف لاكتشاف السلوكيات الشاذة. وبفضل تقنيات السلع، يتم منعك عن رؤية السلوكيات التي توضح لك ما يفعله المستخدمون أثناء دخولهم إلى الشبكة وما يفعلونه على شبكة الإنترنت.
- **دمج شبكة التعلم الخاصة بـ Stealthwatch**. يمكن لهذا الابتكار تمكين جميع الأجهزة بمشاركة البيانات السلوكية وتحسين الذكاء المتعلق بما هو مسموح به، مما يجعله الأمر أسرع وأسهل وأكثر قابلية للتوسعة.
- **تعزيز سياسة defcon بشكل فوري**. يعني ذلك أنه يمكنك الضبط المسبق للسياسات للاستجابة للأحداث الكارثية، مثل البرامج الضارة التي تنتشر في أقل من يوم أو حوادث القرصنة التي تنتشر سريعًا. بضغطة واحدة على أحد الأزرار، يمكنك استدعاء تغييرات سياسة الوصول لكل جهاز على الشبكة لتقييد جميع الاتصالات أو إيقافها حتى يمكن القضاء على هذا التهديد.

- **هوية النقطة الطرفية لأجهزة إنترنت الأشياء والتجزئة التلقائية.** تساعد عمليات فحص أجهزة حافة Cisco في تحديد أكبر مجموعات أجهزة إنترنت الأشياء الطبية في الوقت الحالي، كما أن التقنية تتوسع في العديد من المجالات الأخرى. من خلال التكامل مع التقنيات المتقدمة مثل محرك خدمات الهوية، وأجهزة حافة الشبكة، ستتمكن أجهزة حافة الشبكة من تحديد وتجزئة النقاط الطرفية الأكثر غموضًا تلقائيًا وإضافتها تلقائيًا إلى مقاطع متميزة من الشبكة لحمايتها من الهجوم. ومن ثَم فعندما يقوم أحد العاملين بتشغيل جهاز على الشبكة، يتم التعرف عليه وتصنيفه وإسقاطه في مقطع شبكة الأمان الخاص به.
- **الاحتواء السريع للتهديدات.** تتكامل أجهزة الحافة من Cisco مع محرك خدمات الهوية وTrustSec ومن ثَم فعند اكتشاف Cisco أو أي شركة شريكة لها في مجال دمج التقنيات هجومًا، يمكنهم وضع النقطة الطرفية المسببة للتهديد في مقطع شبكة إما عن طريق أمر من قسم تقنية المعلومات أو تلقائيًا. يتم اكتشاف التهديدات بشكل أسرع والاستجابة لاحتوائها على الفور.
- **اكتشاف البرامج الضارة في حركة مرور البيانات المشفرة.** نظرًا لأن قراصنة الإنترنت يكتشفون المزيد من الطرق الجديدة للوصول إلى الشبكة، تستخدم Cisco قدرتنا على اختبار إطارات الشبكة للتعرف على البرامج الضارة—حتى إذا كانت متضمنة في حركة مرور بيانات مشفرة.
- **حماية السحابة والحماية من البرامج الضارة وبرامج الفدية.** يؤدي التكامل مع Cisco Umbrella الخاصة بالفروع إلى جعل أجهزة الحافة من Cisco جزءًا جوهريًا في حل الحماية من برامج الفدية من Cisco. إذ تمنع المظلة الموظفين من الوصول إلى مواقع الويب الخاصة بالبرامج الضارة أو سيئة السمعة أو المشبوهة. كما تمنع برامج التحكم السرية في البرامج الضارة وبرامج الفدية من الوصول إلى شركائهم، تلك الخطوة التي تُطلب عادةً حتى تعمل تلك البرامج.
- **حماية العمال المتنقلين.** يعد العمال المتنقلون أشيع نقاط انتشار البرامج الضارة نظرًا لأن لديهم حرية الوصول إلى الإنترنت عندما يكونون في أماكن بعيدة. ويمكن مضاعفة حماية عامل حماية Cisco AnyConnect المزود بـ VPN بواسطة الحماية المتقدمة من البرامج الضارة من Cisco وCisco Umbrella للعمل أثناء التنقل، للحفاظ على السلامة أثناء العمل عن بُعد. كما تسمح بالاتصال عبر VPN للعديد من أجهزة حافة Cisco. لن يعمل أيٌ من أنظمة أمان الأجهزة المتنقلة أحادية العامل في بيئة تجارية.
- **تكامل أجهزة الشبكة.** يمتلك قراصنة الإنترنت المزيد من الطرق للانتشار وإضعاف الأنظمة أكثر من مجرد اختراق الثغرات الأمنية بالتطبيقات وأنظمة التشغيل. إذ يهاجمون الأجهزة ومجموعات البرامج الخاصة بأجهزة الشبكات، لذلك يعد تأمين أجهزة الشبكة عنصرًا حيويًا للحفاظ على الأمان. ونظرًا لأنها تعمل على أنظمة التشغيل والتطبيقات، فسوف تستمر في اكتشاف الثغرات الأمنية بأجهزة الشبكة. تتبع Cisco قواعد صارمة فيما يتعلق بتطوير البرامج والأجهزة، وتكملها بالاختبارات المكثفة للمساعدة في ضمان قدرة عملاء Cisco على الاستمرار في العمل على شبكة جديرة بالثقة.

بيانات أعمق ورؤى أسرع

تعمل حافة Cisco بمثابة ثروة معرفية حول ما يحدث بالفعل في عملك، تضم رؤية حول المستخدمين لديك والأجهزة التي يستخدمونها، والتطبيقات التي يصلون إليها. تتمتع بالقدرة على فهم ومعرفة الأجهزة من خلال الأجهزة الموجودة على الشبكة للتكيف تلقائيًا مع التغييرات والاحتياجات. بالإضافة إلى ذلك، فإنها توفر البيانات وفقًا للموقع لتحسين فهم كيفية تفاعل المستخدمين مع البيئة لاتخاذ قرارات أعمال أفضل، ويمكن تقديم أدلة قضائية حول المخاطر لفهم كيفية انتشار تلك المخاطر في الأعمال.

بفضل Cisco IOx Fog Computing، يمكن للحافة تحديد الموقع المثالي إما في المكاتب أو على السحابة، لمعالجة هذه البيانات، مما يسمح للمؤسسة بتحسين الأداء وتقليل التكاليف. توفر تحليلات الموقع الموجودة في تجارب التنقل أثناء الاتصال من Cisco (CMX) تحليلات جيدة من خلال الاتصال عبر Wi-Fi وBluetooth منخفض الطاقة (BLE) لتقديم رؤية واقعية لكيفية تفاعل الأشخاص مع بيئة العمل.

لطالما كانت المؤسسات القائمة على التعامل بين الأعمال التجارية والعملاء (B2N) مثل مؤسسات البيع بالتجزئة والفندقة والمؤسسات التعليمية، قادرة على تحقيق دقة تحديد الموقع على مسافة أقل من متر واحد باستخدام Wi-Fi + BLE وتحقيق زيادة مباشرة في العائدات. وتتضمن بعض الأمثلة، تحقيق Hyatt Regency إيرادات قيمتها 20% بخلاف إيرادات الغرف، وزيادة وقت إقامة العملاء بمعدل ثلاث مرات وتحسُّن تجارب المستخدم بنسبة 80% في المركز التجاري Stary Browar – كل هذا مع استمرارية تقديم تجارب متنقلة مخصصة.

بالإضافة إلى ذلك، توفر Cisco Prime™ رؤية شاملة لجميع المستخدمين النهائيين، وأجهزتهم وتطبيقاتهم المستخدمة على الشبكة. وهذا يسمح بتخطيط أفضل للشبكة وقياس معدل اقتناء التطبيقات وخفض التكاليف.

التكيف في ظل تطور الأعمال من خلال الأتمتة

مع زيادة عدد المستخدمين والأجهزة والمواقع اللازم إدارتها، تصبح الحاجة لأتمتة العمليات والخدمات الجديدة التي تحتاج لإمكانات تنفيذ في أقل من يوم ويوم واحد ضرورةً ملحة. في مناطق الوصول السلكي واللاسلكي، تتيح الأبنية ومراكز البيانات القائمة على تراكب البرامج المنفصلة عن الأجهزة التي تعمل بواسطة الدوائر المتكاملة الخاصة بتطبيقات مخصصة (ASIC):

- المقياس المحسّن
- ضمان الخدمة
- الأمان
- خدمات أخرى لكلٍ من الأجهزة الافتراضية والفعلية والتطبيقات والمستخدمين

قد يؤدي التمثيل الظاهري للشبكة إلى تمكين إدارة السياسة والشبكة وفقًا لنوع المستخدم لبدء التشغيل بسرعة وتخصيص التطبيقات واحتواء التهديدات بسرعة أكبر. ويعد هذا منهجًا مركزيًا للتوجيه للمواقع البعيدة الجديدة خلال دقائق بدلاً من أيام بأمان عبر أي نوع اتصال.

توفر وحدة التحكم الخاصة بتطبيق سياسة البنية الأساسية من Cisco للمؤسسة (APIC-EM) وظيفة التوصيل والتشغيل (PnP) التي يتم التحكم بها مركزيًا وتيسير جودة الخدمة (QoS) للنشر بدون لمس عند الحافة. كما يسمح للتطبيقات الديناميكية لديك منح الأولوية للتطبيقات الحرجة لديك.

توفر Cisco انسيابية ممكَّنة مع البرامج من أجل التخصيص. فمن خلال أنظمة البرامج والأجهزة المدمجة بإحكام، يمكننا تقديم فوائد كبيرة لمؤسستك، وهي ما سيكون واضحًا عند حافة الوصول وWAN. تتضمن المكونات المخصصة لشبكة WANدوائر متكاملة خاصة بتطبيقات مخصصة (ASIC) وبرامج إدارة الشبكة تجعل التمثيل الظاهري لوظائف شبكات المؤسسات من Cisco (Enterprise NFV) واقعًا، حيث يمكنك تشغيل خدمات الشبكة خلال دقائق بدلاً من أشهر. توفر Enterprise NFV إمكانات الحوسبة والتخزين، والبنية الأساسية لإنشاء الشبكات والإدارة، والضمان لتشغيل خدمات الشبكة بحيث يمكنك تقليل التعقيد في الفرع وتمكين خدمات جديدة حسب الطلب عند الحافة.

شهدت المؤسسات انخفاضًا بنسبة 79% في تكاليف النشر باستخدام APIC-EM PnP و85% أسرع والمراقبة باستخدام تطبيقات APIC-EM لشبكة WAN الذكية.

ومع الازدياد الهائل في أعداد المستخدمين والأجهزة المتصلة من جميع أنواع المواقع، يمكن أن تصبح حافة الشبكة عبارة عن تجمعات في كبيرة أو مواقع صغيرة بعيدة. تعمل عروض الهياكل العالمية المزودة بإمكانات التوصيل والتشغيل التلقائية على خفض تكلفة إلحاق جهاز شبكة أو ترقيته مثل المحول أو الموجّه أو نقطة الوصول. تعمل التطبيقات الإضافية على وحدة التحكم على تمكين مراقبة QoS على مستوى الشبكة بالكامل، وحماية حركة مرور البيانات المهمة للأعمال من عملاء النطاق الترددي العريض غير المهمين بسرعة. وتساعد التطبيقات المخصصة مثل تطبيق WAN الذكية (IWAN) في تمكين الإشراف والمراقبة واستكشاف الأخطاء المتعلقة بالأمان والتشفير وتحديد المسار ورؤية التطبيقات والتحكم عبر شبكة WAN وإصلاحها.

بالإضافة إلى ذلك، يقدم برنامج Cisco ONE™ طريقةً قيِّمة ومرنة لشراء البرامج من أجل حافة الشبكة لديك. ففي كل مرحلة من مراحل العمر الافتراضي لمنتجك، يساعدك برنامج Cisco ONE في شراء شبكتك وإدارتها وترقيتها بمزيد من السهولة. إلى جانب تحقيق عائد استثمار هائل مع زيادة استثمارك من خلال استمرار الابتكارات والتحديثات والترقيات المتعلقة بالآلات الظاهرية والفعلية.

الوعي بالتطبيقات والأجهزة

تعد Cisco البائع الوحيد المنوط به تقديم تجربة أفضل من استخدام الأجهزة المحمولة، بالتعاون مع شريكتها الرائدة في مجال صناعة الأجهزة المحمولة، شركة Apple. تعمل تلك الشراكة بين الشركتين على إثراء الذكاء في مجال الشبكات من أجل إمتاع المستخدم بتجربة استخدام Wi-Fi مثالية من خلال التجوال المثالي. بمعنى أن تلك الشراكة تعد سبيلاً أسرع لتوفير تطبيقات مهمة للأعمال على أجهزة Apple iOS في مكان العمل لتحسين إنتاجية الموظفين.

إذ يمكن للمؤسسات أن تتوقع زيادة سرعة التجوال بما يصل إلى ثماني مرات، وزيادة موثوقية إجراء الاتصالات عبر Wi-Fi بنسبة 66% وانخفاض الأعباء الزائدة الناتجة عن إدارة الشبكة بنسبة 50% نظرًا لانخفاض عدد دورات معرفات SSID، كما يمكن للمستخدمين النهائيين إطالة العمر الافتراضي لبطارية أجهزة iOS بنسبة 30%.

على مدى عدة سنوات، قدمت Cisco ابتكارات متعلقة بـ Wi-Fi تتفوق على المعيار القائم وتعمل كنقاط إثبات للمعيار التالي. توفر تقنية Cisco Aironet® اللاسلكية ابتكارات تجارب عالية الكثافة من شأنها تحسين أداء جهاز الموجات الهوائية وتجربة التطبيق. كما احتلت Cisco أيضا منصب الريادة في مجال تقنية التحديد المرن للموجات اللاسلكية التي تعمل على تحسين أداء شبكة Wi-Fi بدون تقييد توفر الموجات اللاسلكية. تتيح هذه الامكانية نقاط وصول لاسلكي للتعرف على الاحتياجات المفاجئة للشبكات اللاسلكية والتكيف مع الشبكة اللاسلكية تلقائيًا لتلبية هذه الحاجة. يعد ذلك مهمًا للغاية في المناطق التي يحتشد بها عدد كبير من المستخدمين ويتصارعون على عرض النطاق الترددي اللاسلكي.

تعتمد الأعمال الرقمية أيضًا على التطبيقات التي تستخدمها لزيادة الإنتاجية والتواصل مع العملاء. لذا تقدم Cisco أدوات التحكم في التطبيقات ورؤيتها والتي تقوم باكتشاف التطبيقات الموجودة عند السلكية واللاسلكية. كما نستخدم التحكم في المسار الذكي لتحديد أفضل مسار عبر WAN مع تحسين التسليم عبر شبكة LAN السلكية أو اللاسلكية لديك، وبذلك يتمتع المستخدمون بأفضل تجربة تطبيق ممكنة.

يمكن للمؤسسات التمتع برؤية عميقة للتطبيقات لأكثر من ١٢٠٠ تطبيق ومنح الأولوية للتطبيقات الأكثر أهمية للعمل بالنقر فوق زر باستخدام البنية APIC-EM والبنية الأساسية Cisco Prime.

يمكن للحافة التحكم في تجربة الموظفين وتحسينها على المستوى الفعلي. إذ يعمل السقف الرقمي من Cisco على زيادة مزايا إنترنت الأشياء لتمتد لتشمل التحويل بين الشبكات المتعددة بالمبنى، ومن بينها:

- الإضاءة
- التدفئة والتبريد
- توزيع الفيديو عبر IP
- أجهزة استشعار إنترنت الأشياء
- وغيرها الكثير، وكل هذا من خلال نظام شبكة أساسي ذكي وآمن

كما يفتح السقف الرقمي الباب أمام الخبرات والكفاءات الجديدة للعاملين، ويقلل من تكاليف تشغيل المرافق.

مصممٌ لملاءمة الاحتياجات المستقبلة بكل صوره

يتضمن نظام التشغيل IOS-XE من Cisco المصمم لملاءمة الاحتياجات المستقبلية، نظام برمجة حسب النموذج واستنادًا إلى المعايير، كما تقوم حافة Cisco بإعداد الشبكة لإضافة وظائف جديدة والتكيف مع التغييرات في البيئة أو العمل، أو الصناعة. وبفضل هذا، تصبح حافة الشبكة مفتوحة وقابلة للبرمجة والتوسعة.

تشهد الحافة تحولاً من الطراز المخصص حسب كل جهاز على حدة حيث تتم إضافة أدوات التحكم في التجزئة والوصول إلى تكوين الشبكة، إلى حل سياسة تشغيل متكامل تلقائي. ففي المستقبل، لن تكون هناك حاجة للإشراف المباشر على الشبكات. إذ ستتمكن من التعبير عن السياسة كما لو أنها مجرد رغبة بسيطة. وعلاوةً على ذلك، يمكنك تحديد نوعية المستخدم أو المجموعات التي يمكنها الدخول إلى مجموعات مميزة معينة من التطبيقات أو البيانات سواءً في المكاتب أم على السحابة. سيتم الإشراف التلقائي على الشبكة لتعزيز هذه السياسة، مع استمرارية السماح بالمرونة الشاملة في المراقبة واستكشاف الأخطاء وإصلاحها ومعالجتها، أو تطبيق خدمات إضافية على حركة مرور بيانات معينة.

كما ستصبح الحافة أيضًا قابلة للبرمجة بالكامل. ويمكن الجمع بين حلول التنسيق المتناغم والحافة باستخدام واجهات برمجة التطبيقات القياسية على حسب الطراز أو البرامج النصية بلغة Python أو أدوات طراز Linux الأخرى. وهذا يجعل طرق دمج الحافة في تطوير البرامج الحديثة أسهل، مما يزيد من السرعة والتخصيص بشكل غير مسبوق.

الابتكارات المتواصلة في مجال حافة الشبكة

في ظل الثورة الهائلة في مجال الاتصال بالإنترنت وما تحمله من فرص ذهبية، بدأت الشركات تدرك أن التحول سيستلزم تغييرات جذرية في البنية الأساسية لديهم وفي قدرتهم على إدارة وتحليل البيانات. ونحن نحتل منصب الصدارة في مسار التحول هذا عن طريق تقديم ابتكارات في مجال البنية الأساسية للشبكة وإدارتها والتحليلات لاستخلاص رؤى قابلة للتنفيذ من البيانات.

وتهدف Cisco إلى الانتقال من مجرد القيام برد الفعل عن طريق اكتشاف المشكلات وإصلاحها إلى القيام بدور استباقي تحضيري حتى الوقت المستقطع في حل المشكلات من أيام إلى دقائق. وسنقوم بذلك من خلال التعامل مع كل جهاز على الشبكة بصفته جهاز استشعار وعنصر معالجة بيانات موزعة. ومن خلال الحصول على البيانات من الأجهزة عند الحافة، وتوزيع المعالجة بشكل أقرب إلى مصدر البيانات، يمكننا إجراء تحليلات في سرعة الخط لإنشاء رؤى يمكن تنفيذها من خلال التعلم.

وبفضل امتلاكها أكبر قاعدة مثبتة وحلول ASIC مخصصة، تحتل Cisco مكانةً فريدة في مجال تصميم الأجهزة والبرامج المحسنة للتحليلات. تسخير قوة القاعدة المثبتة. إن الجمع بين الشبكتين السلكية واللاسلكية في شبكة واحدة يعني أن الذكاء على الحافة قد يساعدك في استكشاف المشكلات وإصلاحها، سواء حدثت تلك المشكلات عند الحافة أو لا، في بضع ثوانٍ. ومع مرور الوقت، يمكن تصحيح المشكلات المحتملة حتى قبل حدوثها. وهذا سيساعد ذلك أقسام تقنية المعلومات في تقديم الخدمة وفقًا لاتفاقية مستوى الخدمة (SLA) الخاص بالشبكة وأداء التطبيقات اللازم في المستقبل.

الخاتمة

نظرًا للاعتماد على حافة الشبكة بهذه الدرجة الكبيرة، يمثل تسليع الاتصال السلكي واللاسلكي بالشبكة LAN وWAN خطرًا قد ينجم عنه اختراقات أمنية وانخفاض الإنتاجية والإيرادات وضياع الفرص ونقص وضوح الرؤية. وتتيح حافة الشبكة من Cisco للمؤسسات تجاوز الأسلوب الجاهز المكبل بالمعايير، عن طريق إثراء الحافة بالذكاء عالي القيمة.

يسمح هذا الأسلوب للمؤسسات بما يلي:

- حماية العمل بواسطة خط دفاع أول قوي
- تقديم تطبيقات للجمهور المستهدف بكل ثقة
- تقديم تجربة سلسة للموظفين في أي مكان
- التواصل مع العملاء لجلب تدفقات إيرادات جديدة
- إدارة أجهزة إنترنت الأشياء بشكل أفضل وتحسين البيئة الفعلية
- توفير رؤية مثالية لما يحدث فعليًا في العمل

لمزيد من المعلومات

لمعرفة المزيد، يرجى زيارة صفحة تقنية Cisco Unified Access على http://www.cisco.com/c/en/us/solutions/enterprise-networks/unified-access/index.html.

08/16 C11-737691-00