# شبكات الجيل التالي: حماية في الحاضر والمستقبل

إن حماية الشبكات التي تم تصميمها للوفاء بمتطلبات الماضي ضد التهديدات التي نشهدها اليوم يجعل الشركات عرضة للاختراق.

تتطور بيئة الحوسبة الخاصة بالشركات تطوراً سريعاً استجابةً للاتجاه المنادي بالترويج الاستهلاكي لتكنولوجيا المعلومات وإمكانية التنقل والحوسبة السحابية. تقدم هذه الاتجاهات فرصاً استراتيجية جديدة في مجال الأعمال – بالإضافة إلى عرض مخاطر ونقاط ضعف جديدة. يتعين على مؤسسات تكنولوجيا المعلومات أن تجد طريقة لحماية أصول الشركات أثناء تمكين الأعمال لتحقيق قيمة هذه الاتجاهات. ويمكن أن يصبح ذلك أكثر تعقيداً مما يجب أن يكون عليه إذا كانت مؤسسة تكنولوجيا المعلومات تدعم شبكة "جيدة بشكلٍ كافٍ". يلقي هذا المستند التقني نظرة على الآثار المترتبة على حماية شبكة منخفضة النفقات الرأسمالية وجيدة بشكلٍ كافٍ مقابل المخاطر التي نشهدها في الوقت الراهن وكيف يمكن لشبكة الجيل التالي أن تدعم بيئة تكنولوجيا المعلومات لتكون أكثر أماناً.

## نموذج نظام أمان الشبكات في الماضي

منذ وقت ليس ببعيد، كان تأمين بيئة تكنولوجيا المعلومات أسهل من تأمينها الآن. وكانت المعلومات الأساسية مثل مواقع المستخدمين والتطبيقات التي كانوا يستخدمونها وأنواع الأجهزة التي كانوا يستخدمونها عبارة عن متغيرات معروفة. بالإضافة إلى ذلك، كانت هذه المعلومات ثابتة إلى حدٍ ما، ولذا نجحت سياسات الأمان في الارتقاء بمستوى الأمان إلى حدٍ معقول. وكانت التطبيقات تعمل باستخدام خوادم مخصصة لذلك في مركز البيانات وتمتعت مؤسسة تكنولوجيا المعلومات بسلطة التحكم في الوصول إلى تلك التطبيقات وقامت بوضع حدود تضمن تطبيق سياسات الأمان. تم تأمين التطبيقات ونقاط النهاية، وتم تقييد الوصول إلى الشبكة. وكان الهدف من هذه الشبكة هو توصيل المستخدمين بموارد تكنولوجيا المعلومات على هيئة عميل/خادم و– في معظم الأحيان – شهدت الشبكة أنماطًا يمكن التنبؤ بها في حركة المرور.

وفي الوقت الراهن، تؤثر اتجاهات الحوسبة المتطورة على تأمين الشبكات بطريقتين رئيسيتين. أولاً، تؤثر هذه الاتجاهات على طريقة تصميم الشبكة. لقد تطورت الشبكة حيث تقوم الأجهزة المحمولة المتعددة والمتنوعة بالاتصال بشبكة الشركة من مواقع مختلفة. تنتقل التطبيقات في حد ذاتها أيضاً – حيث يتم تطبيق تقنية المحاكاة الافتراضية عليها وقد تنتقل بين الخوادم أو حتى بين مراكز البيانات. ويقوم المستخدمون في الوقت نفسه بمد شبكة الشركة من خلال السعي وراء الخدمات السحابية من أجل التطبيقات التعاونية مثل Dropbox و Google Docs. فلم تعد تكنولوجيا المعلومات على علم بالأجهزة المتصلة بالشبكة أو مواقع هذه الأجهزة. ولم يعد التطبيق المستخدم قاصراً على ما تقدمه تكنولوجيا المعلومات فقط. فالبيانات لا تستقر بأمان في مركز البيانات، ولكنها تجتاز البلاد من خلال الهواتف الذكية وأجهزة الكمبيوتر اللوحية وهي توجد بعيداً عن متناول تكنولوجيا المعلومات، في أبعد الآفاق.

أما الاتجاه الثاني الذي يؤثر على أمان الشبكة فيتمثل في ظهور التهديدات المعقدة والمتطورة بشكل متزايد. تعرضّت الشبكات في الماضي إلى هجمات واسعة النطاق. فقد كان قراصنة الإنترنت يقومون بإرسال، على سبيل المثال، مليوني رسالة بريد إلكتروني مزعجة وكانوا يستغلون وجود خطر حتمي أو نقطة ضعف معروفة جيداً ويعتمدون على قيام نسبة مئوية من المتلقين بفتح البريد الإلكتروني والاستسلام لهذا الهجوم.

الوصف الإعلامي من
CSO Custom Solutions Group

مدعم من قبل
cisco

أما الآن، فقد انقلب نموذج الهجوم. فلم يعد قراصنة الإنترنت يستهدفون عدداً كبيراً من الأفراد. حتى أنهم قد لا يسعون وراء نقطة ضعف بارزة. وبدلاً من ذلك، فإنهم يقومون بتنفيذ هجمات موجهة وأكثر تعقيداً. قد يستخدم قراصنة الإنترنت الهندسة الاجتماعية في الحصول على معلومات حول الهدف ثم يقومون بعد ذلك باستغلال ثقة المستخدمين لأحد التطبيقات أو مستخدم آخر لتثبيت برامج ضارة أو لسرقة البيانات. ومقارنةً بالهجمات واسعة النطاق، فإن هذه الهجمات الموجهة للغاية تحظى بفرصة أكبر إن لم يتم اكتشافها إلا بعد نجاح قراصنة الإنترنت في إحداث بعض الأضرار.

## تأمين الشبكة الجيدة بشكلٍ كافٍ

للأسف، فإن هناك تطوراً آخر من شأنه أن يعرقل الجهود التي تبذلها مؤسسات تكنولوجيا المعلومات في الأمان. حيث يشجع بعض المحللون والموردون مؤسسات تكنولوجيا المعلومات على عرض الشبكة باعتبارها سلعة؛ بمعنى آخر، ستفي أية شبكة بالغرض، ولا تحتاج مؤسسات تكنولوجيا المعلومات إلا إلى تنفيذ شبكة جيدة بشكلٍ كافٍ بأقل تكلفة شراء. ولكن أي توفير يتم تحقيقه مُقدماً في التكاليف ينكمش سريعاً بسبب افتقار هذه الشبكات الجيدة بشكلٍ كافٍ إلى نظام أمان متكامل. ونتيجة لذلك، يجب أن تتصدى تكنولوجيا المعلومات لهذه المخاطر بالاستعانة بحلول متعددة النقاط – عن طريق بذل المزيد من الوقت والجهد في نشر الحلول وتكوينها وإدارتها. حيث أن نظام حماية تكنولوجيا المعلومات لا يستطيع أن يتماشى معه، ناهيك عن توقع، المخاطر الأمنية. وحيث إنه لم يتم إدماج الحلول القائمة على نقاط فردية من قبل، فمن الممكن أن يكون تطبيق سياسات الأمان المتوافقة عبر بيئة تكنولوجيا المعلومات بالكامل أمراً صعباً. ومن منطلق دفاعي، كلما زاد السياق الذي تتمتع به تكنولوجيا المعلومات كلما كانت مجهزة بشكل أكبر لإيقاف الهجمات على الشبكة. إن الحاجة إلى الربط بين المعلومات من الأنظمة المختلفة للحصول على السياق بالغ الأهمية يُبطِل الهدف من هذا الإجراء.

وجود شبكة جيدة بشكلٍ كافٍ مزودة بحلول متعددة النقاط يعني وجود شبكة غير مستقرة وهو ما يشكل خطورة أكبر تتسبب في حدوث أوقات تعطل. يمكن أن تنتج أوقات التعطل عن وجود إحدى الثغرات الأمنية أو حدوث اختراق أو عدة اختراقات للنظام. وعند تعطل الشبكة، يتعطل أي شيء أخر، بما في ذلك الأرباح.

## الأسلوب الحديث لتأمين الشبكة

من ناحية أخرى، لا تعد الشبكة الجيدة بشكلٍ كافٍ ومقتضيات الأمان الخاصة بها الخيار الوحيد. فلقد استمرت الابتكارات الخاصة بمجال تأمين الشبكة مواكبة لاتجاهات الحوسبة المتطورة بشكل سريع. حيث تأخذ شبكة الجيل التالي تقنيات المستقبل في الاعتبار وتم تصميمها باستخدام إمكانيات أمان متكاملة للحماية الاستباقية ضد التهديدات المستهدفة والمعقدة. وهذه الحماية هي التي تمكن مؤسسة تكنولوجيا المعلومات من المثابرة بثقة عند متابعة فرص الأعمال الإستراتيجية مثل إمكانية التنقل والحوسبة السحابية.

توفر شبكة الجيل التالي رؤية وتحكم واسعي الانتشار بالإضافة إلى وعي كامل بالمضمون لتوفير الأمان عبر الشبكة، بدءاً من مقر الشركة إلى المكاتب الفرعية، لكلٍ من العاملين من المنزل والعاملين على الأجهزة السلكية أو اللاسلكية أو VPN. يمكن أن تقوم بنية سياسة انتشار الشبكة بإنشاء قواعد أمان وتوزيعها ومراقبتها استناداً إلى لغة سياقية، مثل مَن، وماذا، وأين، ومتى، وكيف. قد تتضمن عملية التطبيق إجراءات مثل حظر الوصول إلى البيانات أو الأجهزة، أو بدء تشفير البيانات. على سبيل المثال، عندما يقوم أحد الموظفين بالاتصال بشبكة الشركة من خلال هاتف ذكي، تقوم الشبكة بالتعرف على الجهاز والمستخدم، بالإضافة إلى الامتيازات الممنوحة لهم. حيث إن محرك السياسة لا يقوم فقط بإنشاء سياسات لكلٍ من الجهاز والمستخدم، بل أيضاً يقوم بمشاركة تلك السياسات مع كافة النقاط على الشبكة، ويقوم على الفور بتحديث المعلومات عند ظهور جهاز جديد على الشبكة.

من الواضح أن سياسات انتشار الشبكة المدمجة تعمل على تسهيل الاستخدام الآمن لسياسات "جلب الجهاز الخاص بك"[1] ، لكن شبكات الجيل التالي يمكنها أيضاً معالجة مخاوف الحماية المتعلقة بالحوسبة السحابية. من خلال نقرة الانتقال عبر شبكة خطوط موزعة ، يمكن للأعمال إعادة توجيه حركة المرور عبر الويب بشكل فعال لفرض سياسات قوية تتعلق بالأمان والتحكم.

***يعاني أي توفير يتم تحقيقه مُقدماً في التكاليف من الانكماش السريع بسبب افتقار هذه الشبكات الجيدة بشكلٍ كافٍ إلى نظام حماية متكامل. ونتيجة لذلك، يجب أن تتصدى تكنولوجيا المعلومات لهذه المخاطر بالاستعانة بحلول متعددة النقاط.***

مدعم من قبل

CISCO

[1] تشير العبارة "أحضر الجهاز الخاص بك" إلى وجود اتجاه جديد حيث يقوم الموظفون من خلاله باستخدام الأجهزة الشخصية الخاصة بهم مثل الهواتف الذكية أو الأجهزة اللوحية للوصول إلى موارد الشركات.

***مع تنفيذ الشبكة ذات النفقات الرأسمالية المنخفضة فإن مؤسسات تخاطر "برفض" التقنيات الناشئة أو الشركات التجارية لأن الشبكة غير قادرة على دعمها.***

مدعم من قبل

CISCO

## الشبكة الجيدة بشكلٍ كافٍ مقابل شبكة الجيل التالي

تقدم شبكة الجيل التالي ما هو أكثر من الأمان المتكامل. لقد تم تطوير شبكة الجيل التالي بشكل إستراتيجي لتتلاءم بشكل أفضل مع المتطلبات الحالية وقد تم تصميمها لتتسع لمعوقات تقنية المستقبل بينما تقوم بتوفير حماية للاستثمارات. وبمعنى آخر، إن شبكة الجيل التالي هي شبكة ديناميكية تقوم بدعم الاتجاهات المتعلقة بإمكانية التنقل والحوسبة السحابية ومشهد التهديد المتغير. كما أنها تقوم أيضاً بتحويل الشبكة إلى إحدى آليات تقديم الخدمة التي تُمكن مديرو التأمين الرئيسيون من "الموافقة" على جهود الأعمال الإستراتيجية المستقبلية.

عند إحصاء التكلفة الإجمالية للملكية (TCO)، يجب أن يكون المدير المسؤول عن الأمن حريصاً على عدم التقليل من قيمة الأعمال التي يمكن الحصول عليها من الفرص الإستراتيجية. مع تنفيذ الشبكة ذات النفقات الرأسمالية المنخفضة فإن مؤسسات تخاطر "برفض" التقنيات الناشئة أو الشركات التجارية لأن الشبكة غير قادرة على دعمها. وذلك يعني "رفض" جلب سياسات الجهاز الخاص بك، و"رفض" الجهود التوسعية الافتراضية لتطبيقات المهام الضرورية للعمل، و"رفض" الخدمات السحابية، و"رفض" الوسائط الغنية. ويتم فقد كافة إجراءات التوفير في التكلفة، والميزة التنافسية، ومزايا الإنتاجية والسرعة بسبب توفير بضعة دولارات عبر الشبكة. وبالرغم من ذلك، يمكن لهذه الفوائد ذاتها موازنة التكلفة الإجمالية لشبكة الجيل التالي الخاصة بالمؤسسة.

فلنلقِ نظرة عن قرب ونقارن كيف تختلف الشبكة منخفضة التكلفة أو الجيدة بشكلٍ كافٍ عن شبكة الجيل التالي، وشبكة تمكين الأعمال:

- **الهدف من الشبكة:** لدى الشبكة الجيدة بشكلٍ كافٍ هدف واحد: وهو توصيل المستخدم بموارد تكنولوجيا المعلومات. قد يكون ذلك مقبولاً في عام 2005 حينما كان المستخدمون يستخدمون أجهزة سطح المكتب التي تتصل بمنافذ إيثرنت. إن شبكة الجيل التالي للمؤسسة هي عبارة عن شبكة موحّدة تتألف من عملاء سلكيين، ولاسلكيين وعن بُعْد وهي تشمل عدة أجهزة، بالإضافة إلى بناء وصول وتحكم في الطاقة. يمكنها أن تخدم عدة أغراض، بما في ذلك توصيل جهاز بجهاز، حسبما يكون ذلك مطلوباً لشبكات استشعار جديدة أو لتطبيقات النسخ الاحتياطي الخاصة بمركز البيانات.
- **الأمان:** مع الشبكة الجيدة بشكلٍ كافٍ،يكون الأمان محكم. وبمعنى آخر، يتألف الأمان من منتجات نقطية لا تكون مدمجة بشكل جيد. لكن شبكة الجيل التالي تقوم بدمج إمكانات الأمان بدءًا من وحدة التخزين المحلية إلى الخدمة السحابية. حيث يعني الدمج تكاليف إدارية أقل وعدد أقل من الثغرات الأمنية.
- **معلومات التطبيق:** تتميز الشبكة الجيدة بشكلٍ كافٍ بعدم معرفتها لنوع التطبيق ونقاط النهاية. حيث تتعامل مع مفهوم البيانات على أنها مجرد بيانات ليس أكثر. بينما تكون شبكة الجيل التالي مدركة لنوع التطبيق ونقاط النهاية. حيث تتكيف مع التطبيق الذي يتم تقديمه وجهاز نقاط النهاية الذي تظهر به.
- **جودة الخدمة:** تم بناء الشبكة الجيدة بشكلٍ كافٍ وفقًا لمعايير QoS الأساسية، التي تستطيع إثبات عدم كفاءتها فيما يتعلق بحركة مرور الفيديو وأجهزة سطح المكتب الافتراضية. تتميز شبكة الجيل التالي بوجود عناصر تحكم مدركة للوسائط لدعم دمج الصوت والفيديو.
- **المعايير:** إن الشبكة الجيدة بشكلٍ كافٍ تستند إلى المعايير دون مخاوف من المستقبل. حيث إن شبكة الجيل التالي لا تدعم فقط المعايير الحالية وإنما تعمل على دفع الابتكارات التي تؤدي إلى المعايير المستقبلية.
- **الضمان:** تأتي الشبكات الجيدة بشكلٍ كافٍ مع استمارة دعم محدود للصيانة وبيان الضمان. يقدم موفرو شبكة الجيل التالي ضمانًا، بالإضافة إلى خدمات ذكية مزودة بإدارة متكاملة.
- **تكاليف الشراء:** قد يكون توفير المال من نسبة النفقات الرأسمالية مقدمًا موازنًا للزيادة في نسبة نفقات التشغيل إذا كان هناك تكاليف دمج أعلى، أو أوقات تعطل أكثر أو ثغرات خطيرة في الحماية. وفي الوقت الذي يقوم فيه موردو الشبكة الجيدة بشكلٍ كافٍ بتقليل هذه التكاليف، يقوم موردو شبكة الجيل التالي بترويج أسلوب للأنظمة لا يقتصر عمله على تقليل تكاليف الشبكات المتعلقة بنفقات التشغيل فقط، ولكنه يقوم أيضًا بدفع تحسينات في خدمات تكنولوجيا المعلومات وفرص أعمال جديدة في مجال الأعمال مما يؤدي إلى زيادة عائد الاستثمار.

***تعتبر عملية تأمين الشبكات المصممة في الماضي بالنسبة لتقنيات الحاضر أمرًا شاقًا. تحتاج تكنولوجيا المعلومات إلى وجود شبكات الجيل التالي بجانبها لتوقع المخاطر والتهديدات المعقدة الناشئة عن الترويج الاستهلاكي لتكنولوجيا المعلومات، وإمكانية التنقل، والحوسبة السحابية.***

مدعم من قبل

CISCO

## بنية الشبكة Borderless Network

لقد وضعت شركة Cisco إطار عمل لشبكة الجيل التالي أطلقت عليه اسم بنية شبكة Borderless Network. وهذا يوضح كيف تم تخطيط الرؤية بعيدة المدى التي تتمتع بها شركة Cisco لتقديم مجموعة جديدة من خدمات الشبكة ولدعم متطلبات الأعمال والمستخدمين النهائيين. تحسن هذه الخدمات من قدرة المؤسسة على الوفاء بالمتطلبات الجديدة والناشئة الخاصة بالمستخدمين وتكنولوجيا المعلومات. تعد خدمات الشبكة الذكية أمرًا أساسيًا في خفض التكلفة الإجمالية للملكية وزيادة قدرة تكنولوجيا المعلومات على تقديم إمكانيات جديدة في قطاع الأعمال.

حيث تهدف شركة Cisco إلى بناء أنظمة متصلة والسماح للعملاء بقضاء وقت أقل أسفل الرفوف للعمل على دمج الشبكة الأساسية عن طريق تقديم مجموعة من خدمات الشبكة التي تحسن قدرة الشبكة على تلبية احتياجات المستخدمين والأعمال.

يوجد مفتاح واحد وراء نجاح شبكات Cisco Borderless Networks وهو إطار العمل Cisco SecureX – نظام حماية يمتد من نقطة النهاية إلى الخدمات السحابية ويوفر السياسة والتحكم عند كل عقدة في الشبكة، بالإضافة إلى إدارة مركزية وأدوات متكاملة للتخطيط المسبق والتكوين وتوزيع السياسة على مستوى الشبكات واستكشاف الأخطاء وإصلاحها.

## إطار عمل Cisco SecureX

يعمل Cisco SecureX على دمج طاقة شبكة Cisco مع الأمان المدرك للسياق لحماية المؤسسة الحالية بغض النظر عن الزمان أو المكان أو كيفية استخدام الأشخاص للشبكة. تم بناء إطار عمل Cisco SecureX على أساس ثلاثة مبادئ تأسيسية:

- **تستخدم سياسة إدراك السياق** لغة وصفية مبسطة خاصة بمجال الأعمال لتحديد سياسات الأمان التي تستند إلى خمس معلمات: هوية الشخص، والتطبيق المستخدم، وجهاز الوصول، والموقع والتوقيت. تقدم سياسات الأمان هذه المساعدة للشركات التجارية من أجل تقديم نظام أمان أكثر فعالية والوفاء بأهداف التوافق مع توفير كفاءة تشغيلية وتحكم بدرجة أكبر.
- **يقوم تطبيق الأمان المدرك للسياق باستخدام** الشبكة ونظام الاستخبارات العالمية لاتخاذ قرارات التنفيذ عبر الشبكة ولتقديم نظام أمان شامل ومتوافق في أي مكان في المؤسسة. تعمل خيارات النشر المرنة، مثل خدمات الأمان المدمجة، أو الأجهزة التي تعمل بشكل مستقل أو خدمات الأمان القائمة على الخدمات السحابية على تقريب الحماية من المستخدم وخفض أحمال الشبكة وزيادة الحماية.
- **تقدم الشبكة ونظام الاستخبارات العالمية** رؤية عميقة لنشاط الشبكة ومشهد التهديدات العالمي من أجل الحصول على حماية سريعة ودقيقة ولإعمال السياسة:
  - > يحصل نظام الاستخبارات المحلية من البنية التحتية الخاصة بشبكة شركة Cisco على بنود للسياق مثل الهوية والجهاز والوضع الأمني والموقع والسلوك لتطبيق الوصول وسياسات تكامل البيانات.
  - > يوفر نظام الاستخبارات العالمية التي تمثل بصمة شركة Cisco التأمين العالمي (Cisco Security Intelligence Operations–SIO) السياق الكامل والمُحدَّث وسلوك التهديدات لتمكين حماية دقيقة في الوقت الفعلي.

يسمح Cisco SecureX للمؤسسات بتبنّي إمكانية التنقل والخدمة السحابية مع حماية أصول الأعمال الهامة. فهو يوفر رؤية وتحكم شاملين على مستوى المستخدم والجهاز وعبر المؤسسة بأكملها. وبالنسبة لمؤسسات تكنولوجيا المعلومات، فإن ذلك يوفر حماية أسرع وأدق من تهديدات من طرف إلى طرف، وحماية دائمة، ونظام الاستخبارات العالمية المتكاملة. تستفيد مؤسسة تكنولوجيا المعلومات من الكفاءة التشغيلية المتزايدة من خلال السياسات المبسطة، وخيارات الأمان المدمجة، والتطبيق التلقائي لإجراءات الأمان.

## الخاتمة (الخلاصة)

تعتبر عملية تأمين الشبكات المصممة في الماضي بالنسبة لتقنيات الحاضر أمرًا شاقًا. تحتاج تكنولوجيا المعلومات إلى وجود شبكات الجيل التالي بجانبها لتوقع المخاطر والتهديدات المعقدة الناشئة عن الترويج الاستهلاكي لتكنولوجيا المعلومات، وإمكانية التنقل، والحوسبة السحابية. تعمل شبكات الجيل التالي المزودة بنظام أمان مدمج وشامل على تسهيل تمكين الأعمال مع استمرار المحافظة على الوضع الأمني المناسب واللازم لطبيعة المهام الحرجة التي تتسم بها أنظمة تكنولوجيا المعلومات الجديدة.

**تعرف على المزيد من الموقع www.cisco.com/go/security.**