نظرة عامة على الجيل التالي من جُدر الحماية من شركة Palo Alto Networks

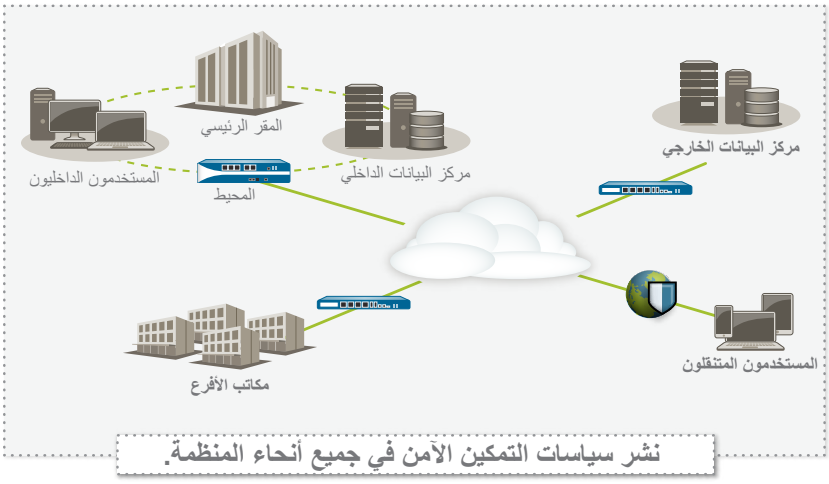
لقد أدت التغييرات الرئيسية في التطبيقات وخصائص التهديدات وسلوك المستخدم والبنية التحتية للشبكة إلى التقليل بشكل تدريجي من الأمان الذي وفرته من قبل جدر الحماية التقليدية المستندة إلى المنافذ. ويصل المستخدمون إلى كافة أنواع التطبيقات باستخدام نطاق من أنواع الأجهزة، وذلك لإنجاز أعمالهم في كثير من الأحيان. في هذه الأثناء، يدفعك توسيع مركز المعلومات والمحاكاة الافتراضية والتنقل والمبادرات المستندة إلى مجموعة النظراء إلى إعادة التفكير في كيفية إتاحة الوصول إلى التطبيق وحماية الشبكة الخاصة بك في نفس الوقت.

تشمل الاستجابات التقليدية محاولة منع جميع البيانات المارة الخاصة بالتطبيقات من خلال قائمة متزايدة من تكنولوجيات point technologies، بالإضافة إلى جدار الحماية، مما قد يعيق أعمالك، أو السماح بجميع التطبيقات وهو يعد أمراً غير مقبول أيضاً بسبب تزايد الأعمال والمخاطر الأمنية. والتحدي الذي يواجهك هو أن جدار الحماية التقليدي المستند إلى المنافذ الخاص بك لا يقدم حلاً بديلاً لأي من الطريقتين، حتى مع منع التطبيقات المضافة بشكل سريع وآمن. لتحقيق التوازن بين السماح بكل شيء ومنع كل شيء، أنت تحتاج إلى تمكين التطبيقات بشكل آمن من خلال استخدام عناصر متعلقة بالأعمال، مثل: هوية التطبيق والأشخاص الذين يستخدمون التطبيق ونوع المحتوى، كمعايير رئيسية لسياسة أمن جدار الحماية.

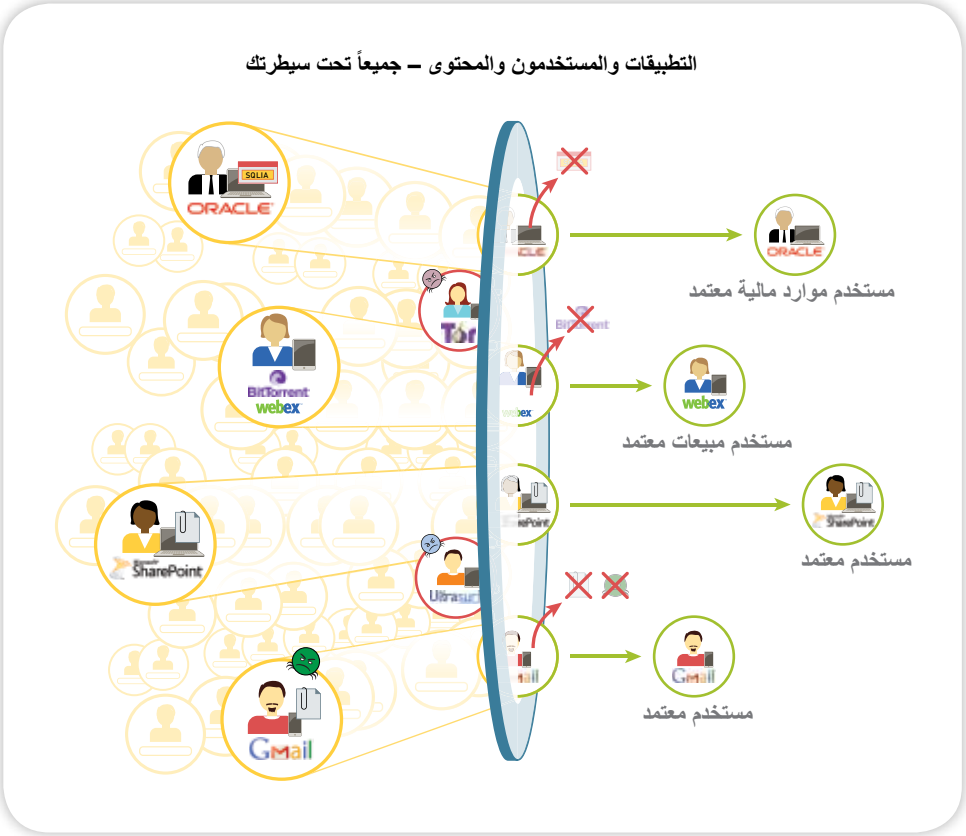
المتطلبات الرئيسية للتمكين الآمن:

- **تحديد التطبيقات، وليس المنافذ.** تصنيف البيانات المارة، بمجرد اصطدامها بجدار الحماية، لتحديد هوية التطبيق، وذلك بغض النظر عن البروتوكول أو التشفير أو أسلوب المراوغة. ثم استخدام هذه الهوية كأساس لكافة السياسات الأمنية.
- **ربط استخدام التطبيق بهوية المستخدم وليس بعنوان IP، وذلك بغض النظر عن الموقع أو الجهاز.** تخدام معلومات المستخدم والمجموعة من أدلة المؤسسات وغيرها من مخازن المستخدم، وذلك لنشر سياسات التمكين المتسقة لجميع المستخدمين بغض النظر عن الموقع أو الجهاز.
- **الاحتجاج على كافة التهديدات - سواء كانت معروفة أو غير معروفة.** منع عمليات استغلال الثغرات الأمنية المعروفة والبرامج الضارة وبرامج التجسس وعناوين URL الضارة أثناء تحليل البيانات المارة، وتوفير الحماية بشكل تلقائي ضد البرامج الضارة المستهدفة بشكل كبير وغير المعروفة من قبل.
- **تبسيط إدارة السياسة.** تمكين التطبيقات بشكل آمن وتقليل الجهود الإدارية من خلال استخدام الأدوات الرسومية سهلة الاستخدام ومحرر السياسة الموحد والقوالب ومجموعات الأجهزة.

قد تساعدك سياسات التمكين الآمن للتطبيقات في تحسين الوضع الأمني، بغض النظر عن موقع النشر. في المحيط، يمكنك التقليل من تأثير التهديدات من خلال منع مجموعة كبيرة من التطبيقات غير المرغوب بها، ثم فحص التطبيقات المسموح بها بحثًا عن التهديدات - سواء كانت معروفة أو غير معروفة. في مركز البيانات – سواء كان تقليدياً أو افتراضياً، يؤدي تمكين التطبيقات إلى ضمان استخدام تطبيقات مركز البيانات من قبل المستخدمين المصرح لهم فقط، وذلك لحماية المحتوى من التهديدات وللتعامل مع التحديات الأمنية التي أدخلتها الطبيعة الديناميكية للبنية التحتية الافتراضية. ويمكن حماية المكاتب الفرعية لمؤسستك والمستخدمين عن بعد باستخدام نفس مجموعة سياسات التمكين التي تم نشرها في المقر الرئيسي، وبذلك تضمن اتساق السياسة.



paloalto NETWORKS
the network security company™



تمكين التطبيقات لتفعيل الأعمال

إن التمكين الآمن للتطبيقات مع الجيل التالي من جدر الحماية من شركة Palo Alto Networks يساعدك في إدارة أعمالك والتعامل مع المخاطر الأمنية المتعلقة بالعدد المتزايد بشكل سريع من التطبيقات التي تعبر الشبكة الخاصة بك. فمن خلال تمكين التطبيقات للمستخدمين أو مجموعات المستخدمين، سواء كانوا محليين أو متنقلين أو عن بعد، وحماية البيانات المارة من التهديدات المعروفة وغير المعروفة، يمكنك تحسين الوضع الأمني الخاصة بك وتنمية أعمالك.

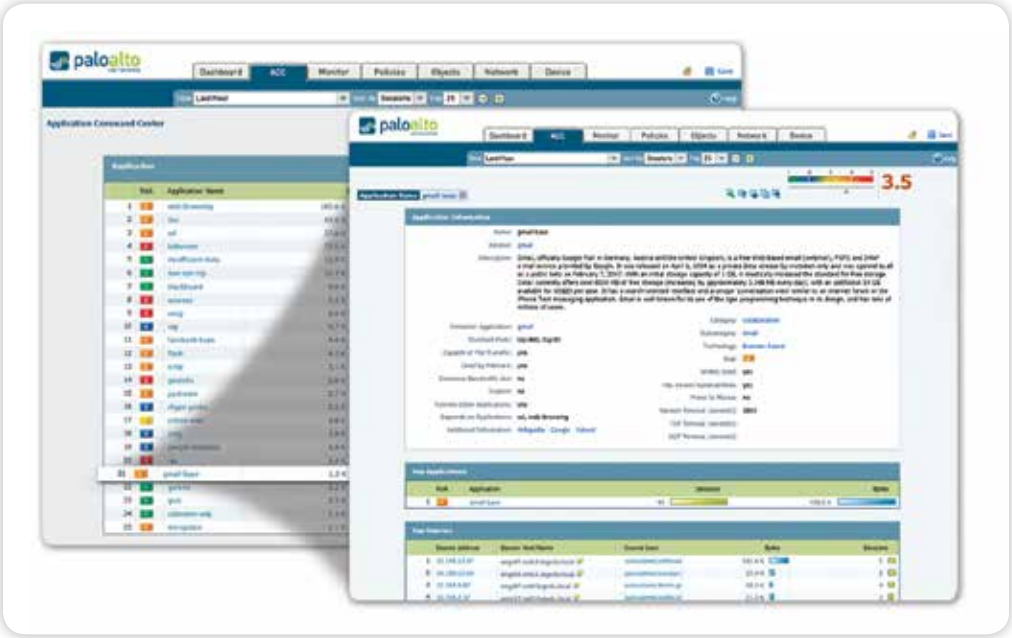
- **تصنيف جميع التطبيقات، عبر جميع المنافذ، في كل الأوقات.** يُعد التصنيف الدقيق للبيانات المارة هو جوهر أي جدار حماية، ونتيجة لذلك يصبح أساساً للسياسة الأمنية. فاليوم يمكن للتطبيقات تخطي جدار الحماية المستند إلى المنافذ بسهولة؛ عن طريق التنقل بين المنافذ باستخدام البروتوكولات SSL وSSH، أو التسلل عبر المنفذ 80، أو استخدام المنافذ غير القياسية. يعالج App-ID قيود الرؤية الخاصة بتصنيف البيانات المارة التي تعاني منها جدر الحماية التقليدية من خلال استخدام العديد من آليات التصنيف مع تدفق مرور البيانات، وذلك حالما يلاحظها جدار الحماية، لتحديد بدقة هوية التطبيقات التي تعبر الشبكة الخاصة بك، بغض النظر عن المنفذ أو التشفير (البروتوكولات SSL أو SSH) أو تقنيات المراوغة المستخدمة. وأصبحت المعرفة الدقيقة للتطبيقات التي تعبر من خلال الشبكة الخاصة بك، ليس فقط المنفذ والبروتوكول، بمثابة الأساس لكافة القرارات المتعلقة بالسياسة الأمنية الخاصة بك. يتم بشكل تلقائي تصنيف التطبيقات غير المحددة، والتي تشكل عادة نسبة صغيرة من البيانات المارة ولكن في نفس الوقت تنطوي على نسبة كبيرة من المخاطر المحتملة، من أجل الإدارة النظامية - التي قد تشمل التحكم في السياسة وفحصها أو التحليل الجنائي للمخاطر أو إنشاء App-ID مخصص أو التقاط حزمة من أجل تطوير App-ID من شركة Palo Alto Networks.

- **دمج المستخدمين والأجهزة، وليس عناوين IP فقط، في السياسات.** يُعد إنشاء وإدارة السياسات الأمنية التي تستند إلى التطبيق وهوية المستخدم، بغض النظر عن الجهاز أو الموقع، هو وسيلة أكثر فعالية من الاعتماد فقط على المنفذ وعنوان IP لحماية الشبكة الخاصة بك. إن الدمج مع مجموعة كبيرة من مستودعات بيانات مستخدمي المؤسسات يوفر هوية مستخدم Microsoft Windows أو Mac OS X أو Linux أو Android أو iOS الذي يصل إلى التطبيق. وتتم حماية المستخدمين المتنقلين أو الذين يعملون عن بعد بسلاسة باستخدام نفس السياسات المتسقة المستخدمة على الشبكة المحلية أو شبكة الشركة. إن الجمع بين رؤية أنشطة تطبيقات المستخدم والتحكم فيها يعني أنه يمكنك بشكل آمن تمكين استخدام Oracle أو BitTorrent أو Gmail أو غيرها من التطبيقات التي تعبر الشبكة الخاصة بك، بغض النظر عن المكان الذي يصل المستخدم إليها منه أو كيفية وصوله إليها.

- **الوقاية ضد كافة التهديدات - سواء كانت معروفة أو غير معروفة.** لحماية الشبكة الحديثة اليوم، عليك أن تتعامل مع مزيج من الاختراقات والبرمجيات الضارة وبرامج التجسس المعروفة، هذا بالإضافة إلى التهديدات المستهدفة غير المعروفة تماماً. وتبدأ هذه العملية بالتقليل من مساحة الهجوم عبر الشبكة من خلال السماح بتطبيقات معينة ورفض جميع التطبيقات الأخرى، سواء بشكل ضمني من خلال إستراتيجية رفض ما دون ذلك أو من خلال سياسات واضحة. بعد ذلك، يمكن تطبيق منع التهديدات المنسق على كافة البيانات المارة المسموح به لمنع مواقع البرامج الضارة المعروفة واستغلال الثغرات الأمنية والفيروسات وبرامج التجسس واستعلامات DNS الضارة بتمريرة واحدة. يتم تحليل وتحديد البرامج الضارة غير المعروفة المخصصة أو غيرها بشكل فعال من خلال تنفيذ الملفات غير المعروفة وملاحظة ما يزيد على 100 سلوك ضار بشكل مباشر في بيئة آلية تحديد الصلاحيات الافتراضية. عند اكتشاف برنامج ضار جديد، يتم إنشاء توقيع للملف المصاب والبيانات المارة المتعلقة الخاصة بالبرنامج الضار بشكل تلقائي وإرساله إليك. ويستخدم التحليل الخاص بمنع جميع التهديدات تطبيق كامل وسياق بروتوكول، وذلك لضمان العثور على التهديدات دائماً حتى إذا حاولت الاختباء من الأمن في الأنفاق أو المحتوى المضغوط أو على المنافذ غير القياسية.

مرونة النشر والإدارة

تتوفر وظيفة التمكين الآمن للتطبيقات إما في نظام أساسي للجهاز محدد الغرض أو في عامل تصميم افتراضي. عندما تقوم بنشر العديد من جدر الحماية من شركة Palo Alto Networks، إما في جهاز أو عوامل تصميم افتراضية، يمكنك استخدام البانوراما (Panorama)، وهو عرض اختياري للإدارة المركزية للحصول على رؤية لنماذج البيانات المارة ونشر السياسات وإنشاء التقارير وإرسال تحديثات المحتوى من موقع مركزي.



رؤية التطبيقات: اعرض نشاط التطبيق في تنسيق واضح وسهل القراءة. قم بإضافة وحذف عوامل التصفية لمعرفة المزيد حول التطبيقات ووظائفها والأشخاص الذين يستخدمونها.

التمكين الآمن للتطبيقات: الطريقة الشاملة

يحتاج التطبيق الآمن إلى طريقة شاملة لتأمين الشبكة الخاصة بك ولتنمية أعمالك، وتبدأ هذه الطريقة تبدأ بالمعرفة المتعمقة للتطبيقات الموجودة على الشبكة الخاصة بك، وهوية المستخدم، بغض النظر عن النظام الأساسي أو الموقع، ونوع المحتوى الذي يحمله التطبيق، إن وجد. ومع المعرفة الشاملة بنشاط الشبكة، يمكنك إنشاء سياسات أمنية هامة تستند إلى عناصر التطبيق والمستخدم والمحتوى المتعلقة بالأعمال الخاصة بك. إن موقع المستخدمين ونظمهم الأساسية ومكان نشر السياسة المحيط أو مركز البيانات التقليدي أو الافتراضي أو المكتب الفرعي أو المستخدم عن بعد لا تحدث جميعها فارقا فيما يتعلق بكيفية وضع السياسة. يمكنك الآن تمكين أي تطبيق وأي مستخدم وأي محتوى بأمان.

المعرفة الشاملة تعني سياسات أمنية أكثر حزما

تُقر أفضل الممارسات الأمنية بأن المعرفة الشاملة بما يوجد على الشبكة الخاصة بك يعد أمراً مفيداً في تنفيذ سياسات أمنية أكثر حزماً. فعلى سبيل المثال: معرفتك الدقيقة بالتطبيقات التي تعبر شبكتك، وذلك خلافاً للمجموعة الأكبر من البيانات المارة التي تستند إلى المنافذ، تمكن المسئولين من السماح بتطبيقات محددة لتمكين الأعمال الخاصة بك ومنع التطبيقات غير المرغوب بها. إن معرفة هوية المستخدمين، وعدم الاكتفاء بعنوان IP الخاص بهم، يضيف معيارا آخرا للسياسة والذي يمكنك من أن تكون أكثر دقة في تعيين السياسة الخاصة بك.

- باستخدام مجموعة فعالة من أدوات الرؤية الرسومية، يتمكن المسئولون من الحصول على صورة أكثر شمولا لنشاط التطبيق والتأثير الأمني المحتمل وتمكينهم من اتخاذ قرارات مبنية على معرفة تخص السياسة. يتم تصنيف التطبيقات بشكل مستمر وعندما تغيير حالتها، ويتم تحديث الملخصات الرسومية بشكل فعال وعرض المعلومات في واجهة سهلة الاستخدام مستندة إلى الويب.
- يمكن فحص التطبيقات الحديثة أو غير المألوفة سريعاً بنقرة واحدة لعرض وصفاً للتطبيق وخصائصه السلوكية وهوية الأشخاص الذين يستخدمونه.
- إن الرؤية الإضافية لفئات URL والتهديدات ونماذج البيانات تقدم صورة كاملة وشاملة لنشاط الشبكة.
- يتم تصنيف التطبيقات غير المعروفة، والتي تشكل عادةً نسبة صغيرة على كل شبكة ولكن في نفس الوقت تنطوي على نسبة كبيرة من المخاطر المحتملة، وذلك من أجل تحليلها لتحديد ما إذا كانت تطبيقات داخلية، مثل: التطبيقات التجارية التي لم يتم تحديدها بعد أو التهديدات.

تمكين التطبيقات وتقليل المخاطر

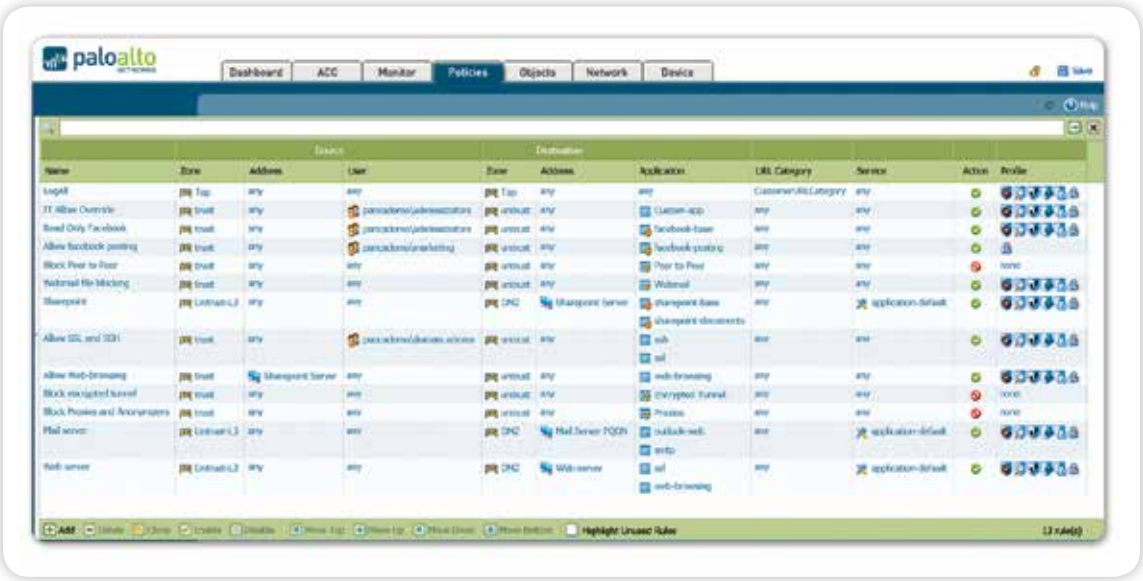
يستخدم التمكين الآمن للتطبيقات معايير خاصة بقرار السياسة والتي تشمل التطبيق/وظائف التطبيق والمستخدمين والمجموعات والمحتوى كوسيلة لتحقيق التوازن بين تقييد الأعمال من خلال رفض كافة التطبيقات وبين البديل الذي ينطوي على نسبة كبيرة من المخاطر من خلال السماح بكافة التطبيقات.

في المحيط، الذي يشمل المكاتب الفرعية والمستخدمين المتنقلين وعن بعد، تركز سياسات التمكين على تحديد جميع البيانات المارة، ثم السماح بشكل انتقائي للبيانات المارة بناءاً على هوية المستخدم، ثم فحص البيانات المارة بحثا عن التهديدات. قد تشمل أمثلة السياسة:

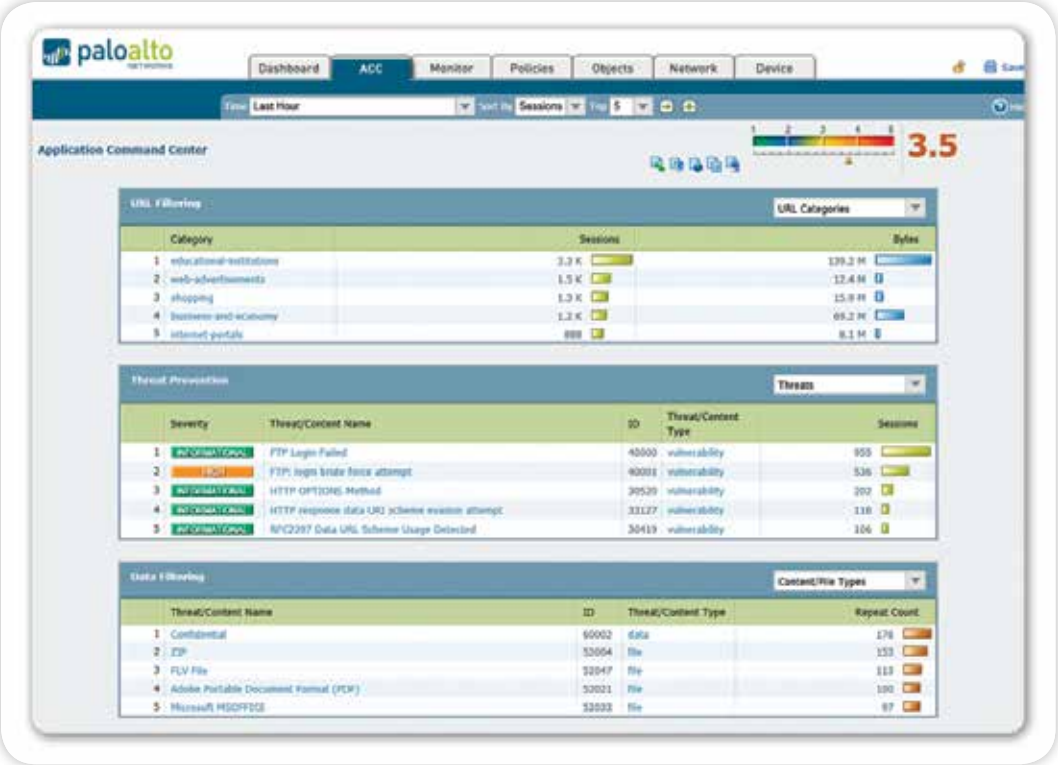
- قصر استخدام بريد الويب والرسائل الفورية على بعض المتغيرات المختارة؛ فك تشفير المتغيرات التي تستخدم بروتوكول SSL وفحص البيانات المارة بحثا عن الاختراقات وتحميل الملفات غير المعروفة على WildFire للتحليل وإنشاء التوقيع.
- السماح بتطبيقات الوسائط المتدفقة ومواقع الويب، ولكن مع استخدام QoS ومنع البرامج الضارة للحد من التأثير على تطبيقات VoIP ولحماية الشبكة.
- التحكم في Facebook من خلال السماح لجميع المستخدمين "بالتصفح"، ومنع جميع ألعاب Facebook والمكونات الإضافية الاجتماعية، والسماح بالنشر على Facebook بغرض التسويق فقط. فحص جميع البيانات المارة الخاصة بـ Facebook بحثا عن البرامج الضارة أو الاختراقات.
- التحكم في التصفح عبر الانترنت من خلال السماح للبيانات المارة إلى مواقع الويب الخاصة بالأعمال وفحصها، ومنع الوصول إلى مواقع الويب غير المتعلقة بالعمل، و"الإشراف" على الوصول إلى المواقع المشكوك بها من خلال صفحات المنع المخصصة.
- فرض الأمن المناسب من خلال نشر نفس السياسات بشفافية إلى جميع المستخدمين سواء كانوا محليين أو متنقلين أو عن بعد باستخدام GlobaIProtect™.
- استخدام إستراتيجية رفض ما دون ذلك الضمنية أو منع التطبيقات غير المرغوب بها بشكل واضح، مثل: P2P وأساليب المراوغة أو البيانات المارة من بلدان معينة، للتقليل من البيانات المارة الخاصة بالتطبيقات والتي تقوم بإدخال مخاطر أمنية ومخاطر تهدد الأعمال.

في مركز البيانات - التقليدي أو الافتراضي أو مزيج من كل منهما - تركز أمثلة التمكين على تأكيد التطبيقات والبحث عن التطبيقات المخادعة وحماية البيانات.

- عزل مستودع رقم بطاقة الائتمان المستند إلى Oracle في المنطقة الأمنية الخاصة به، والتحكم في الوصول إلى المجموعات المالية، ودفع البيانات المارة عبر المنافذ القياسية وفحص البيانات المارة بحثا عن الثغرات الأمنية في التطبيق.
- تمكين مجموعة تكنولوجيا المعلومات فقط من الوصول إلى مركز البيانات باستخدام مجموعة ثابتة من تطبيقات الإدارة عن بعد (مثل: SSH وRDP وTelnet) عبر المنافذ القياسية.
- السماح لفريق الإدارة فقط باستخدام Microsoft SharePoint Administration، والسماح لجميع المستخدمين بالوصول إلى Microsoft SharePoint Documents.



محرر السياسة الموحد: يمكن المظهر والسمات المألوفة من الإنشاء والنشر السريع للسياسات التي تتحكم في التطبيقات والمستخدمين والمحتوى.



المحتوى ورؤية التهديدات: اعرض نشاط نقل عنوان URL والتهديدات والملف/البيانات في تنسيق واضح وسهل القراءة. قم بإضافة وحذف عوامل التصفية لمعرفة المزيد حول العناصر الفردية.

حماية التطبيقات المُمَكَّنَة

إن التمكين الآمن للتطبيقات يعني السماح بالوصول إلى تطبيقات محددة، ثم استخدام سياسات معينة لمنع الاختراقات المعروفة والبرامج الضارة وبرامج التجسس - سواء كانت معروفة أو غير معروفة، والتحكم في نقل الملفات أو البيانات ونشاط التصفح عبر الإنترنت. ويتم التعامل مع أساليب مراوغة التهديدات الشائعة، مثل: التنقل بين المنافذ والمرور عبر الأنفاق، من خلال تنفيذ سياسات منع التهديدات باستخدام سياق البروتوكول والتطبيق الذي يتم إنشاؤه بواسطة أدوات فك التشفير في App-ID. وفي المقابل، تتبع حلول UTM طريقة تستند إلى المخازن لمنع التهديدات، مع كل وظيفة وجدار حماية وIPS وAV وتصفية URL وجميع عمليات فحص البيانات المارة دون مشاركة أي سياق، مما يجعلهم أكثر عرضة لسلوك المراوغة.

- **منع التهديدات المعروفة: نظام IPS وبرامج الشبكة للحماية من الفيروسات/التجسس.** يمكنك تنسيق التوقيع الموحد ومحرك الفحص المستند إلى التدفق من حماية الشبكة الخاصة بك ضد مجموعة واسعة من التهديدات. يقوم نظام منع الاختراق (IPS) بمنع استغلال الثغرات الأمنية بالشبكة والتطبيقات وتجاوزات سعة المخزن المؤقت وهجمات قطع الخدمات (DoS) وفحص المنافذ. تقوم برامج الحماية من الفيروسات/التجسس بمنع الملايين من متغيرات البرامج الضارة، وأية بيانات مارة خاصة بالأوامر والتحكم ناتجة عن برامج ضارة، وفيروسات PDF، والبرامج الضارة المختبأة في الملفات المضغوطة أو البيانات المارة عبر الانترنت (HTTP/HTTPS المضغوط). ويؤدي فك تشفير SSL المستند إلى السياسة عبر أي تطبيق على أي منفذ في حمايتك من البرامج الضارة التي تتحرك عبر تطبيقات SSL المشفرة.
- **منع البرامج الضارة المستهدفة غير المعروفة: Wildfire.** يتم تحديد وتحليل البرامج الضارة غير المعروفة أو المستهدفة بواسطة WildFire، الذي يقوم بتشغيل وملاحظة الملفات غير المعروفة في بيئة آلية تحديد الصلاحيات الافتراضية المستندة إلى مجموعة النظراء. يقوم WildFire برصد ما يزيد على 100 سلوك ضار ويقدم النتائج فوراً إلى المسئول في شكل تنبيه. وتوفر المشاركة الاختيارية في WildFire حماية معززة وتسجيل وتقديم تقارير. وكمشترك، ستتوفر لك الحماية في غضون ساعة عند العثور على أحد البرامج الضارة في أي مكان في العالم، مما يوقف بشكل فعال انتشار البرامج الضارة الجديدة قبل أن تؤثر عليك. وكمشترك، يمكنك أيضاً الوصول إلى التسجيل وتقديم التقارير الخاصين بـ WildFire المتكامل وواجهة برمجة التطبيقات (API) لإرسال العينات إلى مجموعة نظراء WildFire للتحليل.

- **تحديد المضيفين المصابين بالروبوت.** يقوم App-ID بتصنيف كافة التطبيقات عبر جميع المنافذ، بما في ذلك أيه معلومات مارة غير معروفة، والتي قد تعرض الشبكة الخاصة بك لأمور غير طبيعية أو تهديدات. يتعلق التقرير السلوكي الخاص بشبكة الروبوت بالبيانات المارة غير المعروفة واستعلامات DNS وURL ومجموعة متنوعة من سلوكيات الشبكة غير التقليدية وذلك للكشف عن الأجهزة التي من المحتمل إصابتها بالبرامج الضارة. ويتم عرض النتائج في شكل قائمة بالمضيفين المحتمل إصابتهم والذين يمكن التحقق منهم كأعضاء محتملين في شبكة الروبوت.
- **تقييد نقل الملفات والبيانات غير المصرح بها.** تمكن مزايا تصفية البيانات المسئولين من تنفيذ السياسات التي ستقلل من المخاطر المتعلقة بنقل الملفات والبيانات غير المصرح بها. يمكن التحكم في نقل الملفات من خلال البحث داخل الملف (بدلاً من النظر فقط على امتداد الملف) لتحديد ما إذا كان سيتم السماح بإجراء النقل أم لا. قد يتم منع الملفات القابلة للتنفيذ، والتي يتم العثور عليها عادة في التنزيلات العابرة، وبذلك تتم حماية الشبكة من انتشار البرامج الضارة غير المرئية. إن مزايا تصفية البيانات يمكنها كشف والتحكم في أنماط البيانات السرية (بطاقة الائتمان أو أرقام الضمان الاجتماعي، ذلك بالإضافة إلى نماذج الجمارك).
- **التحكم في تصفح الإنترنت.** يسمح مشغل التصفية URL المخصص والمتكامل للمسئولين بتطبيق سياسات تصفح الإنترنت متعدد المستويات واستكمال سياسات رؤية والتحكم في التطبيق وحماية المؤسسة من نطاق كبير من المخاطر القانونية والتنظيمية والإنتاجية. بالإضافة إلى ذلك، يمكن الاستفادة من تصنيفات URL في السياسات لتوفير المزيد من التحكم في فك تشفير SSL أو QoS وغيرها من قواعد التحكم.

الإدارة والتحليل المستمران

تُقر أفضل الممارسات الأمنية أن المسئولين يحققون بشكل فعال التوازن بين إدارة جدر الحماية، في حالة الجهاز الواحد أو مئات الأجهزة، وبين الحفاظ على الفعالية والفحص والتحليل وتقديم التقارير عن الحوادث الأمنية.

- **الإدارة:** يمكن إدارة كل نظام أساسي من شركة Palo Alto بشكل فردي من خلال واجهة سطر الأوامر (CLI) أو من خلال واجهة كاملة المميزات مستندة إلى المتصفح. ومن أجل النشر على نطاق واسع، يمكن ترخيص إجراء بانوراما (Panorama) ونشرها كحل إداري مركزي يمكنك من الموازنة بين التحكم العالمي المركزي وبين الحاجة إلى مرونة السياسة المحلية باستخدام المميزات، مثل: القوالب والسياسة المشتركة. يسمح لك الدعم الإضافي للأدوات المستندة إلى المقاييس، مثل: بروتوكول SNMP وواجهات برمجة التطبيقات (API) المستندة إلى نقل الحالة التمثيلية (REST)، بالاندماج مع أدوات إدارة الطرف الثالث. سواء في حالة استخدام واجهة الويب أو البانوراما (Panorama) للجهاز، فإن مظهر وسمات الواجهة تكون مطابقة، وذلك لضمان عدم وجود منحنى التعلم عند الانتقال من واحد إلى آخر. ويمكن للمسئولين استخدام أي من الواجهات المقدمة لإحداث التغييرات في أي وقت دون الحاجة إلى القلق بشأن مسائل المزامنة. يتم دعم الإدارة المستندة إلى الدور من خلال جميع وسائل الإدارة، مما يسمح لك بتعيين المزايا والوظائف لأفراد معينين.
- **تقديم التقارير:** يمكن استخدام التقارير المعرفة سابقاً كما هي أو مخصصة أو جمعها معاً في تقرير واحد من أجل ملائمة المتطلبات المحددة. ويمكن تصدير جميع التقارير إلى تنسيق CSV أو PDF ويمكن تنفيذها وإرسالها بالبريد الإلكتروني في مواعيد محددة وفقا لجدول زمني.
- **التسجيل:** إن تصفية السجل في الوقت الحقيقي تسهل من عملية التحقيق الجنائي السريع في كل جلسة تعبر الشبكة الخاصة بك. ويمكن تصدير نتائج تصفية السجل إلى ملف CSV أو إرسالها إلى خادم syslog لإجراء تحليل إضافي أو أرشيفي دون اتصال بالإنترنت.

أجهزة محددة الغرض أو نظم أساسية افتراضية

تقدم Palo Alto Networs خطاً كاملاً من النظم الأساسية للأجهزة محددة الغرض بداية من PA-200، المصمم تصميمها لمكاتب المؤسسات التي تعمل عن بعد، ووصولا بـ PA-5060، والذي تم تصميمه لمراكز البيانات عالية السرعة. تعتمد بنية النظام الأساسي على محرك برامج العبور الواحد وتستخدم معالجة مخصصة الوظائف للشبكات والأمن ومنع التهديدات والإدارة، وذلك لتقديم الأداء الذي تتوقعه. وتتوفر نفس وظائف جدار الحماية التي تقدمها النظم الأساسية للأجهزة في جدار الحماية الافتراضي VM-Series، مما يسمح لك بتأمين بيئات الكمبيوتر الافتراضية والمستندة إلى مجموعة النظراء باستخدام نفس السياسات المستخدمة في المحيط الخاص بك أو في جدر الحماية الخاصة بالمكاتب التي تعمل عن بعد.

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

paloalto NETWORKS
the network security company™