WILDFIRE – جلوگیری خودکار هک و تروجان جدید بسیار گریزان

سرویس تحلیل تهدید مبتنی بر ابر Palo Alto Networks® WildFire™ پیشرفته‌ترین موتر تحلیل و پیشگیری صنعتی در مقابل سوءاستفاده بدافزارهای جدید و هک بسیار گریزان است. این سرویس، رویکرد چندتکنیکی منحصر به فرد با تحلیل پویا و استاتیک، روش‌های نوآورانه یادگیری ماشین و محیط تحلیل متداول پیشگامانه برای شناسایی و جلوگیری از تهدیدات انحرافی است.

سرویس تحلیل تهدید WildFire

- شناسایی بدافزارها و نرم‌افزارهای مخرب با استفاده از ترکیب منحصر به فرد تحلیل پویا و استاتیک، تکنیک‌های یادگیری ماشین‌های جدید و اولین محیط تحلیل مواد خالص صنعتی.
- پیشگیری از تهدیدات ناشناخته در کمتر از ۵ دقیقه از اولین کشف در هر نقطه از جهان بدون نیاز به پاسخ دستی.
- ایجاد ایمنی در مقابل بدافزارهای ناشناخته و تقسیم اطلاعات در زمان حقیقی در میان تقریباً ۱۷۰۰۰ مشترک.
- ارائه تحلیل و محتوای تهدید با ارتباط بالا با AutoFocus.

امروزه، سازمان‌ها باید با بازار بدافزار رقابت کنند و ابزارهای مخرب توسعه‌دهندگان فروش یا اجاره اطلاعات را استخراج کرده و به کلیه دسته‌های حملات دسترسی پیدا کنند. در عین حال، روش‌های پیشگیری پیشرفته نیز تغییر کرده است، به حملات اجازه می‌دهد تا از روش‌های شناسایی میرا عبور کنند. در حال حاضر حتی دشمنان با مهارت پایین می‌توانند حملات منحصر به فردی انجام دهند که قادر به رفع روش‌های شناسایی و پیشگیری از تهدید سنتی هستند و مستلزم مداخلات انسانی هستند تا نتوان آنها را در مقابل حجم حملات ناشناخته امروزه ارزیابی کرد.

WildFire معادله را برای دشمنان تغییر می‌دهد و هر پلت فرم شبکه‌های Palo Alto به سنسور توزیع شده و مقررات اجرایی تبدیل می‌شود تا به طور موفقیت‌آمیزی از ترویج بدافزار جدید جلوگیری شود. در محیط WildFire، تهدیدات منهدم می‌شود، اطلاعات استخراج شده و پیشگیری‌ها به صورت خودکار در پلت‌فرم امنیتی نسل بعد شبکه‌های Palo Alto به مدت ۵ دقیقه پس از اولین کشف در هر نقطه از جهان انجام می‌شود.

شناسایی ناشناخته با رویکرد روش چندگانه منحصر به فرد

WildFire فراتر از روش‌های سنتی مورد استفاده برای شناسایی تهدیدهای ناشناخته است و مزایای چهار روش مستقل برای کشف وفاداری بالا و مقاوم در برابر فرار را به همراه دارد:

- تحلیل پویا- فایل‌هایی که در محیط مجازی ساخته شده‌اند به طور ویژه ردیابی کرده و از بین می‌برد، و امکان شناسایی سوءاستفاده بدافزار را با استفاده از صدها ویژگی رفتاری فراهم می‌کند.
- تحلیل استاتیک- تشخیص بسیار مؤثر بدافزارهای مخرب که تلاش می‌کنند تا از تحلیل پویا فرار کنند و همچنین شناسایی فوری انواع بدافزارهای موجود.
- یادگیری ماشین- استخراج هزاران ویژگی منحصر به فرد هر فایل، آموزش مدل یادگیری ماشین پیش‌بینی برای شناسایی نرم‌افزارهای مخرب جدید- که صرفاً با تحلیل استاتیک و پویا امکان‌پذیر نیست.
- تحلیل مواد خام- تهدیدات انحرافی به طور خودکار به سخت افزار محیطی برای انفجار فرستاده می‌شود، قابلیت دشمن برای راه‌اندازی روش های تحلیلی ضد-VM به طور کامل از بین می‌رود.

این چهار روش منحصر به فرد با هم، دیوار آتش را قادر می‌سازند تا بدافزارهای ناشناخته را شناسایی کرده و از کارایی بالا و مثبت کاذب نزدیک به صفر بهره می‌برد.

ارکستراسیون[1] خودکار پیشگیری

هنگامی که سو استفاده کاربر یا بدافزار توسط کاربر دیوار آتش کشف می‌شود، سرویس حفاظت از ثبات به طور خودکار ۵ دقیقه پس از اولین کشف در هر نقطه جهان توسط دیوار آتش برای کلیه مشترکین اعمال می‌شود. این حفاظت‌ها بدست آمده و در

[1] . Orchestration

میان تقریباً ۱۷۰۰۰ کاربر دیوار آتش به اشتراک گذاشته می‌شود که بزرگترین شبکه حسگر توزیع‌شده در این صنعت است که بر شناسایی و جلوگیری از تهدیدات ناشناخته تمرکز دارد. دیوار آتش نیز مرکز ارزیابی پیشگیری مرکزی برای پلت‌فرم امنیتی نسل بعد شبکه‌های Palo Alto است که امکان اجرای کنترل‌های جدید را در اختیار شما قرار می‌دهد:

- پیشگیری از تهدید برای جلوگیری از فعالیت بدافزارها، سوءاستفاده‌ها و فرمان و کنترل (ضد- C2 و پاسخ مبتنی بر DNS).
- فیلتر URL با PAN-DB برای پیشگیری از URLهای مخرب تازه کشف شده.
- سرویس اطلاعات تهدید متضاد AutoFocus™، امکان استخراج، همبستگی و تحلیل اطلاعات تهدید که ارتباطات بالا و زمینه را فراهم می‌کند.
- حفاظت پیشرفته نقطه پایانی Traps™ و سرویس امنیتی Aperture™ SaaS برای تعیین زمان واقعی تعیین حکم و پیشگیری از تهدید.
- ادغام با شرکای فناوری برای تعیین حکم در خدمات شخص ثالث با API دیوار آتش.

پیشرفته‌ترین محیط تحلیل تروجان

دیوار آتش سالانه نوآوری پیشگامانه برای ارائه پیشرفته‌ترین محیط تحلیل در صنعت را ارائه می‌دهد، که دقیق‌ترین کشف تهدیدهای ناشناخته موجود امروزه را فراهم می‌کند. موتور دیوار آتش بر اساس دو جزء اصلی است:

- ایجاد سفارش مجازی: به منظور جلوگیری از استفاده از نرم‌افزار شبیه‌سازی منبع باز که معمولاً از فرار بی‌بهره‌اند، دیوار آتش مجازی ایمن به روش‌های تحلیل ضد-VM می‌پردازد که برای جلوگیری از تشخیص در تحلیل نرم‌افزارهای مخرب

سنتی محیط سفارش مجازی ارائه شده است که چارچوب انعطاف‌پذیری را برای تشخیص پیشرفته و قابلیت مقاومت در دیوار آتش بعدی را ارائه می‌دهد.

- تحلیل مواد خام: پیچیده‌ترین تهدیداتی را که به طور کامل قادر به نابودی‌شان نیستیم، می‌توان با بررسی در محیط مجازی پیشرفته مشاهده کرد. برای رفع این دسته جدید حملات پیشرفته، دیوار آتش به طور خودکار می‌تواند با استفاده از موتور تحلیل مواد، تهدیدات پیشرفته را در سیستم‌های سخت‌افزاری واقعی تحلیل کند. در حال حاضر، حتی بیشتر تهدیداتی که فرار می‌کنند را می‌توان به طور قطعی شناسایی و جلوگیری کرد.

در محیط تحلیل نرم‌افزارهای مخرب، دیوار آتش محتوای مشکوک را در سیستم‌عامل‌های Windows® XP، Windows 7، Android® و macOS® با دید کامل به فرمت‌های رایج مورد سوء استفاده مانند EXE، DLL، ZIP و PDF به عنوان اسناد Microsoft® Office، فایل‌های Java®، Android APKs، اپلت‌های Adobe® Flash® و لینک‌هایی با پیام‌های ایمیلی اجرا می‌کند. دیوار آتش فایل‌ها را با رفتارهای مخرب بالقوه شناسایی کرده و بر اساس اقدامات خود محکوم می‌کند.

- دید رفتا کاملاً مخرب- تهدیدات در ترافیک کلیه برنامه‌ها از جمله ترافیک وب، پروتکل‌های ایمیل (IMAP،SMTP ، POP) و FTP، بدون در نظر گرفتن درگاه‌ها یا رمزنگاری شناسایی می‌شود.
- تغییرات ساخته شده برای میزبان- کلیه فرایندها برای اصلاحات برای میزبان مشاهده می‌شود، از جمله شواهد بهره‌برداری، مکانیزم پایداری، رمزنگاری داده‌ها (ransomware) یا روش‌های تخریب سیستم.
- ترافیک شبکه مشکوک- تحلیل کلیه فعالیت‌های شبکه تولید شده توسط فایل مشکوک انجام می‌شود، از جمله ایجاد مهاجم، دانلود نرم‌افزارهای مخرب مرحله بعدی، بازدید دامنه‌های کم اعتبار، کشف شبکه و سایر موارد.

- تشخیص ضد تحلیل- نظارت بر روش‌های مورد استفاده توسط نرم‌افزارهای مخرب پیشرفته برای جلوگیری از تحلیل مبتنی بر VM، مانند تشخص اشکال‌زدا، تشخیص مجازی، تزریق کد به فرایندهای قابل اطمینان، غیرفعال کردن ویژگی‌های امنیتی مبتنی بر میزبان و سایر موارد.

اطلاعات تهدید، تحلیل و همبستگی

در ترکیب با دیوار آتش، سازمان‌ها می‌توانند از AutoFocus برای ارائه هدفمندتر با ارتباطات و زمینه بالا استفاده کنند. AutoFocus توانایی شکار را در تمام داده‌های استخراج شده از دیوار آتش و همچنین تهدیدات شخص ثالث را با استفاده از موتور پیوند اطلاعات تهدید MineMeld™ فراهم می‌کنند. این به کاربران اجازه می‌دهد تا شاخص‌های مصالحه (IoCs) و نمونه‌های هوش انسانی تیم تحقیقاتی تهدید واحد ۲۴ در قالب برچسب‌ها هماهنگ شوند. دیوار آتش و AutoFocus تصویر کاملی از تهدیدات ناشناخته‌ای ارائه می‌دهند که سازمان و صنعت شما را مورد هدف قرار داده‌اند و با استفاده از موارد زیر قابلیت شما را برای در نظر گرفتن عمل سریع افزایش می‌دهند

- به‌روزرسانی خودکار لیست‌های دینامیکی خارجی در دیوار آتش نسل بعدی شبکه‌های Palo Alto.
- استخراج خودکار شاخص‌های مصالحه برای راه‌حل‌های شخص ثالث از طریق STIX™، TAXII™ و API.

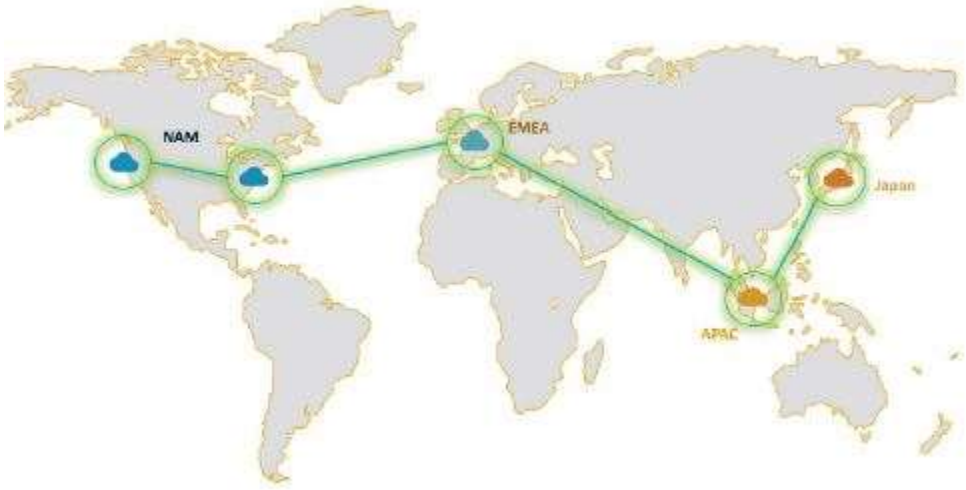
این اقدامات مستلزم دخالت انسان نیست و هزینه افزودن کارکنان امنیتی ویژه را کاهش می‌دهد.

معماری مبتنی بر ابر مقیاس‌پذیر، امن

معماری مبتنی بر ابر منحصر به فرد دیوار آتش از شناسایی و پیشگیری تهدید ناشناخته در مقیاس وسیع در سراسر شبکه، نقطه پایان و ابر پشتیبانی می‌کند. مشتریان بدون در نظر گرفتن تأثیر عملکرد بر دیوار آتش می‌توانند این سرویس را به عنوان بخشی

از پلت‌فرم امنیتی نسل بعد شبکه‌های Palo Alto مورد استفاده قرار دهند. دیوار آتش در حالت‌های استقرار چندگانه‌ای در دسترس است که حتی سخت‌ترین قوانین حفظ حریم خصوصی یا مقررات محلی را شامل می‌شوند، از جمله:

- تحویل ابر سراسری: فایل‌ها به ابر سراسری دیوار آتش ارسال می‌شوند، مقیاس و سرعت ارائه می‌شود و هر مشتری شبکه‌های Palo Alto قادر است به سرعت این سرویس را فعال کند که شامل نسل‌های بعدی دیوار آتش، سری‌های VM، ارائه ابرهای عمومی، روزنه و تله.
- تحویل ابر خصوصی: دستگاه دیوار آتش دستگاه محلی است که کلیه انفجارات تهدید، استخراج اطلاعات و حقاظت را انجام می‌دهد اما قابلیت دریافت به روزرسانی‌های ابر سراسری را برای حفظ حریم خصوصی مشتریان یا الزامات قانونی حفظ می‌کند.
- تحویل ابر ترکیبی: شما می‌توانید مزیت‌های ابر سراسری و خصوصی را با انتخاب ارسال فایل‌های حساس به ابر خصوصی ترکیب کنید در حالی که محتوای دیگر توسط ابر سراسری تحلیل می‌شود.
- زیربنای ابر سراسری: کاربران از حفاظت خودکاری استفاده می‌کنند که از طریق ابر سراسری بدون نیاز به ارسال محتویات خارج از مرزهای خود بدست می‌آید و اجازه می‌دهد تا حریم خصوصی حفظ شود و مقیاس با توجه به منافع آن رعایت شود.



ورود یکپارچه، گزارش و دادرسی قانونی

دریافت یکپارچه کاربران دیوار آتش در حوادث مخرب از طریق رابط مدیریت PAN-OS®، مدیریت امنیت شبکه Panorama™، AutoFocus و پرتال دیوار آتش ثبت، تحلیل و مشاهده می‌شود، و تیم را قادر می‌سازد تا رویدادهای مشاهده شده را به سرعت در شبکه‌هایشان بررسی و مرتبط کند. این عمل کارکنان امنیتی را قادر می‌سازد تا اطلاعات داده شده مورد نیاز برای تحقیقات و پاسخ‌های حادثه را سریعاً شناسایی و اقدام کنند، از جمله:

- تحلیل دقیق هر فایل مخرب ارسال شده به دیوار آتش در سراسر محیط‌های سیستم عامل چندگانه از جمله فعالیت‌های مبتنی بر وب و شبکه.
- اطلاعات دوره‌ای مرتبط با تحویل فایل مخرب از جمله منبع، مقصد، برنامه، کاربر، URL و سایر ویژگی‌ها.
- دسترسی به نمونه اصلی مخرب برای مهندسی معکوس، با PCAPهای کامل دوره‌های تحلیل پویا.
- API باز برای یکپارچه‌سازی با ابزار امنیتی شخص ثالث مانند سیستم‌های اطلاعاتی امنیتی و مدیریت رویداد (SIEM).

پلت‌فرم امنیت نسل بعدی

دیوار آتش در پلت‌فرم امنیتی نسل بعد شبکه‌های Palo Alto ساخته شده است، از تهدیدات شناخته شده و ناشناخته پیش از آسیب‌رسانی جلوگیری می‌کند، از جمله:

- دیدار کامل در تمام ترافیک شبکه، از جمله تلاش‌های بی‌نظیر برای جلوگیری از تشخیص، مانند استفاده از درگاه‌های غیر استاندارد با رمزنگاری SSL.
- کاهش سطح حمله با کنترل‌های امنیت مثبت برای جلوگیری از انتشار ویروس.
- پیشگیری از تهدید خودکار شناخته شده با دیوار آتش نسل بعدی، پیشگیری از تهدید، فیلتر URL، تله‌ها و نفوذ، دفاع در مقابل سوء استفاده های شناخته شده، نرم‌افزارهای مخرب، URLهای مخرب و فعالیت فرمان و کنترل.
- شناسایی و پیشگیری از تهدیدناشناخته با دیوار آتش، از جمله تحلیل تهدید با ارتباطات و زمینه بالا از طریق سرویس AutoFocus.

نتیجه روش منحصر به فرد، حلقه بسته برای جلوگیری از حملات سایبری، اطمینان از آن که همه آنها شناخته شده و توقف در سراسر چرخه عمر حمله است.

حفظ حریم خصوصی فایل‌های شما

اولویت ما امنیت و حریم خصوصی اطلاعات مشتری است. زیرساخت دیوار آتش به طور مستقیم توسط شبکه‌های Palo Alto اداره می‌شود، بهترین شیوه استاندارد و محرمانه صنعت برای امنیت است و برای حسابرسی SOC 2 به طور منظم مورد ارزیابی قرار می‌گیرد. شما می‌توانید اطلاعات بیشتری را درباره مشخصات خصوصی دیوار آتش پیدا کنید.

الزامات دیوار آتش

- PAN-OS 4.1+
- تحلیل DF، Java، Office و APK مستلزم PAN-OS 6.0+ است.
- تحلیل Adobe Flash و صفحه وب مستلزم PAN-OS 6.1+ است.

اطلاعات مجوز

اشتراک ابر سراسری دیوار آتش ارائه می‌دهد:

- محیط‌های تحلیل مجازی ویندوز XP، ویندوز ۷، macOS و Android OS.
- به‌روزرسانی امضاهای خودکار در هر پنج دقیقه برای بدافزارهای جدید و سوءاستفاده‌هایی که توسط نمونه‌های مشترک دیوار آتش برای ابر سراسری دیوار آتش. امضا شامل امضاهای ضد ویروس مبتنی بر فایل، امضای دامنه (DNS) و امضای URL است. امضای URL مستلزم اشتراک PAN-DB است.
- پشتیبانی از فایل‌های PE (EXE، DLL و سایر موارد)، انواع فایل‌های Microsoft Office، فایل‌های PDF، فایل‌های Flash، برنامه‌های جاوا (JAR وCLASS)، Android APK، باینری‌های macOS (mach-O، DMG، PKG و بسته‌های نرم‌افزاری) و تحلیل ارتباطات با پیام‌های ایمیلی. این شامل پشتیبانی برای محتوای فشرده (ZIP) و رمزگذاری (SSL) است.
- تحلیل نمونه‌های انتخاب شده در محیط تحلیل مواد خام که توسط سیستم دیوار آتش تعیین شده است.
- قابلیت دیوار آتش پایه به عنوان ویژگی استاندارد در کلیه پلت‌فرم‌های شبکه‌های Palo Alto که در PAN-OS 4.1 یا بالاتر اجرا می‌شوند در دسترس هستند و مجموعه محدود ویژگی‌های دیوار آتش را تنظیم می‌کنند، از جمله:

- محیط‌های تحلیل مجازی ویندوز XP و ویندوز ۷.
- ارسال خودکار انواع فایل‌های EXE و DLL، شامل فایل‌های فشرده (ZIP) و رمزگذاری (SSL).

حفاظت خودکار که با به روز رسانی محتوا پیشگیری تهدید به طور منظم (مجوز پیشگیری از تهدید)

آدرس: یوسف آباد- میدان جهاد- خیابان بیستون- خیابان فتحی شقاقی- پلاک ۹۳- طبقه دوم - واحد ۵
تلفن:۱-۸۸۳۵۳۴۰۰-۰۲۱
فکس: ۸۹۷۸۴۲۷۱