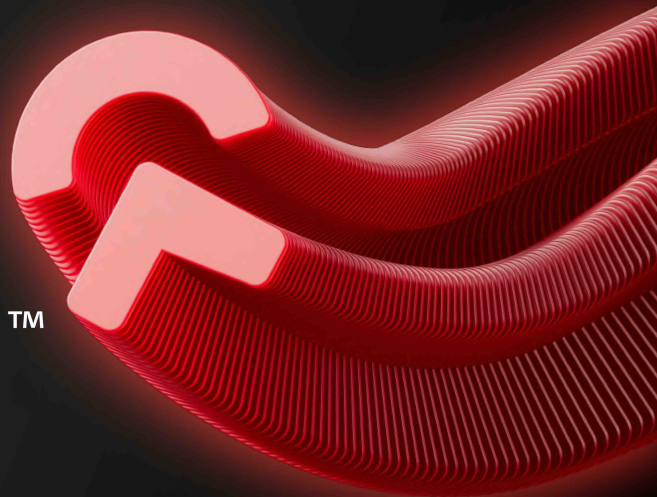


PT APPLICATION FIREWALL™

به صورت هوشمند
از برنامه‌های تجاری خود محافظت کنید



"Positive Technologies به عنوان بزرگترین اپراتور امنیت سایبری روسیه فعالیت میکند و بسیاری از زیرساخت‌های مهم روسیه در بخش دولتی و بانکی و مخابراتی از محصولات آن استفاده میکنند."

گزارش Gartner Magic Quadrant برای فایروال‌های برنامه‌های وب (۲۰۱۵)

تقریباً هر شرکت مدرن از صدها برنامه وب، موبایل یا ERP برای پیشبرد عملیات خود استفاده می‌کند. اما با افزایش تعداد این برنامه‌ها، تعداد آسیب‌پذیری‌های امنیتی موجود در آن‌ها نیز افزایش می‌یابد که می‌تواند برای آسیب رساندن به کسب‌وکار شما بهره‌بردار شود. گزارش Verizon Data Breach Investigation Report (DBIR) ۲۰۱۴ نشان می‌دهد که در سال گذشته ۳۵٪ از نفوذهای امنیتی شامل حملات علیه برنامه‌های وب بوده که نسبت به سال ۲۰۱۲، ۱۴٪ افزایش داشته است. همچنین، حملات به برنامه‌های وب اصلی‌ترین عامل نقض داده‌ها بوده‌اند، و پس از آن جاسوسی سایبری، نفوذ به سیستم‌های POS و سوء استفاده داخلی قرار دارند.

+ چرا این مهاجمان موفق هستند؟ واقعیت این است که اکثر تهدیدات امنیتی برنامه‌ها ناشی از اشتباهات توسعه‌دهندگان است که با اسکریپت‌های امنیتی سنتی، IDS یا فایروال‌ها قابل حل نیستند:

+ مهاجمان اغلب از آسیب‌پذیری‌های روز صفر بهره‌برداری می‌کنند، که تحلیل بر پایه امضا را منسوخ و نیاز به راهکارهای انطباقی، خودآموز و تحلیل رفتاری را تأیید می‌کند.

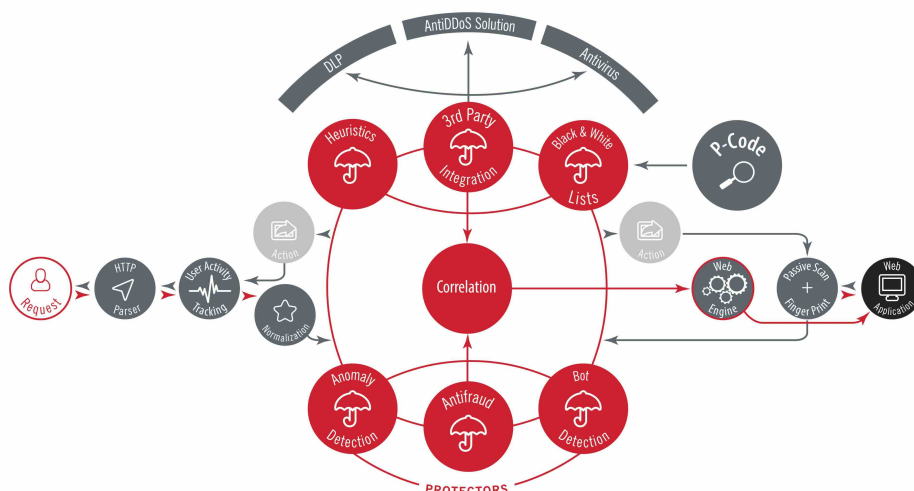
+ برنامه‌های شرکتی مدرن از زبان‌ها، پروتکل‌ها و فناوری‌های مختلفی استفاده می‌کنند و شامل راهکارهای سفارشی و کدهای شخص ثالث هستند. حفاظت از این برنامه‌ها نیاز به تحلیل دقیق ساختار برنامه، الگوهای تعامل کاربران و بستر استفاده دارد.

+ فایروال‌های مدرن با هزاران حادثه مشکوک مواجه می‌شوند. متخصصان امنیتی زمان کافی برای بررسی دستی همه این حوادث به منظور شناسایی تهدیدات واقعی را ندارند. نیاز مبرم به مرتب‌سازی، رتبه‌بندی و تجسم هوشمند رویدادهای امنیتی به صورت خودکار وجود دارد.

+ حتی آسیب‌پذیری‌های شناخته‌شده نیز نمی‌توانند بلافاصله اصلاح شوند؛ رفع آسیب‌پذیری‌های سیستم‌های ERP یا بانکداری الکترونیکی ممکن است ماه‌ها به طول بینجامد. یک سیستم امنیت برنامه باید دارای مکانیزمی برای کاهش اثرات نقض‌ها در حین رفع کد توسط توسعه‌دهندگان باشد.

+ Secure SDL می‌تواند به طور چشم‌گیری هزینه اشتباهات را کاهش دهد، مشروط بر اینکه این اشتباهات در مراحل اولیه کدنویسی اصلاح شوند، اما یافتن راه‌حل‌های خودکار موثر برای تحلیل کد کار دشواری است.

PT Application Firewall™: Modules and Engines



مزایای کلیدی

مکانیزم‌های حفاظت برتر – تطبیق سریع و پیوسته با سیستم‌های شما

به جای استفاده از روش کلاسیک مبتنی بر امضا، فایروال برنامه کاربردی PT™ ترافیک شبکه، لاگ‌ها و فعالیت کاربران را تحلیل کرده و یک مدل آماری در لحظه از عملکرد عادی برنامه ایجاد می‌کند؛ این مدل برای شناسایی رفتار غیرعادی سیستم استفاده می‌شود. به همراه سایر مکانیزم‌های حفاظتی، این روش تضمین می‌کند که ۸۰٪ از حملات روز صفر بدون نیاز به تنظیمات خاص مسدود می‌شوند.

کاهش تلاش‌های عملیاتی و تمرکز بر تهدیدات اصلی

PT AF™ تلاش‌های نامرتب برای حمله را فیلتر کرده، حوادث مشابه را گروه‌بندی کرده و زنجیره‌های حمله را شناسایی می‌کند – از جاسوسی تا سرقت داده یا ایجاد درب پشتی. به جای دریافت هزاران پیام بالقوه تهدید، متخصصان امنیت اطلاعات فقط ده‌ها پیام مهم دریافت می‌کنند.

P-Code: مسدودسازی آتی

تکنیک وصله مجازی ما به شما امکان می‌دهد تا از برنامه محافظت کنید، حتی قبل از اینکه کد ناامن اصلاح شود. اما اکثر WAF‌ها برای ایجاد هر وصله مجازی به کار دستی نیاز دارند. فناوری منحصر به فرد PT برای تحلیل کد منبع با مکانیزم تولید اکسپلویت (P-Code)، شناسایی خودکار آسیب‌پذیری‌ها و ایجاد وصله مجازی برای فایروال برنامه کاربردی PT™ را فراهم می‌کند. همین مازول P-Code اطلاعات دقیقی درباره کد نادرست به توسعه‌دهندگان ارائه می‌دهد و هزینه‌های اصلاح و تست را به شدت کاهش می‌دهد.

حذف بای پس‌های امنیتی

PT AF™ داده‌ها را با توجه به پشته فناوری سرور محافظت‌شده پردازش کرده و پروتکل‌های JSON، XML و دیگر پروتکل‌های معمول در پورتال‌ها و برنامه‌های موبایل مدرن را تحلیل می‌کند. این ویژگی از بیشتر روش‌های دور زدن فایروال مانند HPP، HPC و دستکاری افعال محافظت می‌کند.

آیا شرکت شما تحت حمله قرار گرفته است؟

شبکه و محیط خارجی خود را بررسی کنید

برای درخواست آزمایشی رایگان Positive Technologies، با ما تماس بگیرید.

PT@SafeNEST.ir

درباره Positive Technologies

Positive Technologies یکی از ارائه‌دهندگان برتر راهکارهای ارزیابی آسیب‌پذیری، مدیریت تطبیق و تحلیل تهدیدات به بیش از ۳,۰۰۰ مشتری در سطح جهانی است. راهکارهای ما به‌طور یکپارچه در سراسر کسب‌وکار شما کار می‌کنند: حفاظت از برنامه‌ها در حال توسعه، ارزیابی آسیب‌پذیری‌های شبکه و برنامه‌ها، اطمینان از تطبیق با الزامات قانونی و مسدودسازی حملات در زمان واقعی. تعهد ما به مشتریان و پژوهش‌ها به Positive Technologies شهرتی به عنوان یکی از معتبرترین مراجع در امنیت SCADA، بانکداری، مخابرات، برنامه‌های وب و ERP داده است و در گزارش IDC به عنوان سریع‌ترین شرکت در حال رشد در مدیریت امنیت و آسیب‌پذیری در سال ۲۰۱۲ شناخته شده است. برای اطلاعات بیشتر درباره Positive Technologies، به سایت ptsecurity.com مراجعه کنید.



منبع: پیش‌بینی جهانی مدیریت امنیت و آسیب‌پذیری IDC 2013-2017 و سهم فروشندگان در سال ۲۰۱۲، سند شماره 242465، آگوست ۲۰۱۳. بر اساس رشد درآمد سالانه در سال ۲۰۱۲ برای فروشندگانی با درآمد بیش از ۲۰ میلیون دلار.

© Positive Technologies 2016. Positive Technologies و لوگوی آن، علائم تجاری یا علائم ثبت‌شده Positive Technologies هستند. تمام علائم تجاری دیگر ذکر شده متعلق به صاحبان مربوطه هستند.

شرکت فناوری ارتباطات آشیانه امن ارائه‌دهنده خدمات زیرساخت و امنیت شبکه می‌باشد که دارای مجوز توزیع‌کننده و نمایندگی فروش و خدمات محصولات شرکت PT در ایران است همچنین دارای تیمی مجرب در ارائه خدمات امنیت شبکه مانند تست نفوذ و ارزیابی امنیتی و راه‌اندازی و راهبری مرکز عملیات امنیت و اقدامات و محصولات بومی جهت شناسایی حملات فیشینگ و حفاظت از برندهای معتبر می‌باشد.



شرکت Positive Technologies

پیشرو در صنعت امنیت سایبری و ارائه‌دهنده جهانی راهکارهای امنیت اطلاعات است. مأموریت ما: حفاظت از کسب‌وکارها و منابع مختلف در برابر حملات سایبری و آسیب‌های غیرقابل تحمل. بیش از ۳,۳۰۰ سازمان در سراسر جهان از فناوری‌ها و خدمات توسعه‌یافته توسط شرکت ما استفاده می‌کنند.