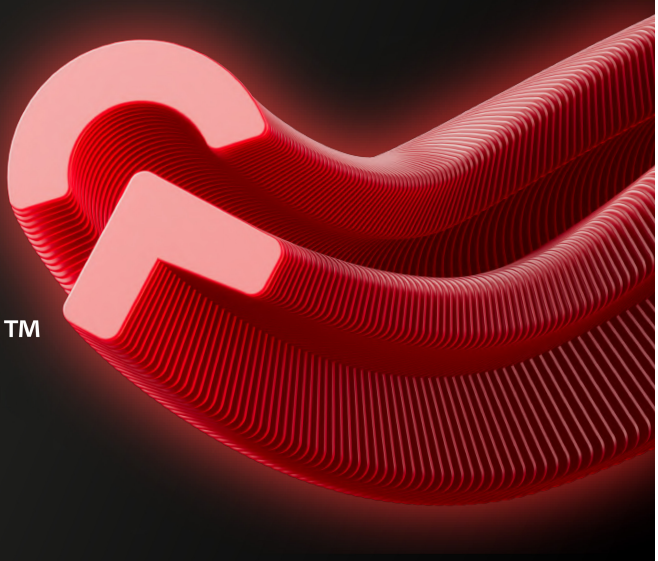
positive technologies



PT APPLICATION FIREWALL ™

به‌صورت 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 می‌توانند برای آسیب رساندن به کسب‌وکار شما بهره‌برداری شوند. 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 اسکنرهای 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.

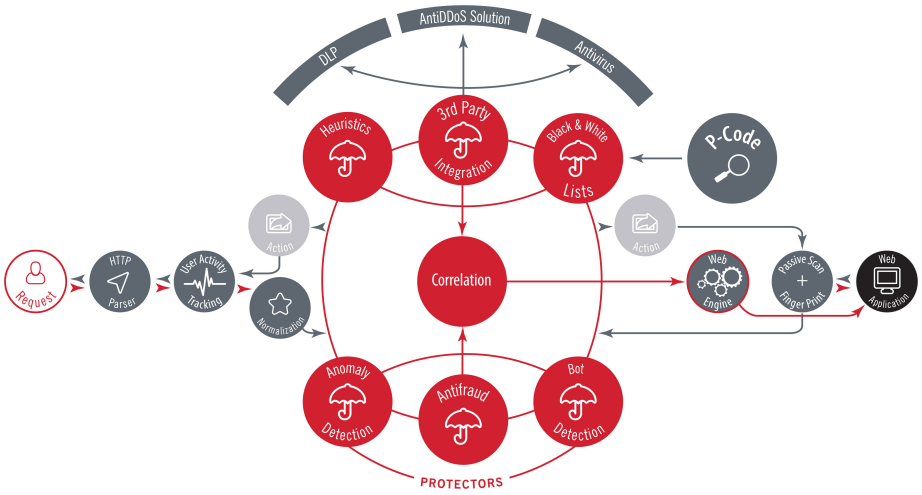
+ برنامه‌های شرکتی مدرن از زبان‌ها، پروتکل‌ها و فناوری‌های مختلفی استفاده می‌کنند و شامل راهکارهای سفارشی و کدهای شخص ثالث هستند. حفاظت از این برنامه‌ها نیاز به تحلیل دقیق ساختار برنامه، الگوهای تعامل کاربران و بستر استفاده دارد.

+ 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 به‌صورت 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 نقص‌ها 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 نامرتبط 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 آنی

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 ماژول P-Code اطلاعات دقیقی درباره کد نادرست به توسعه‌دهندگان ارائه می‌دهد و هزینه‌های اصلاح و تست را به شدت کاهش می‌دهد.

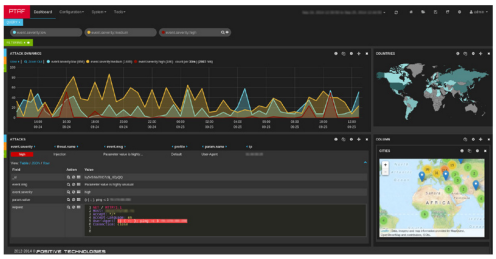
حذف بای‌پس‌های امنیتی

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.

محافظت‌سفارشی‌سازی‌شده

با بیش از ۱۰ سال تحقیق در حوزه امنیت و یک پایگاه دانش گسترده از آسیب‌پذیری‌ها، کارشناسان Positive Technologies تجربه گسترده‌ای در محافظت از شرکت‌ها با اندازه‌ها و صنایع مختلف به دست آورده‌اند. هر صنعت ویژگی‌ها و نیازهای خاص خود را دارد که برای امنیت عملی حیاتی هستند. هر استقرار فایروال برنامه کاربردی PT™ شامل پیکربندی‌هایی برای برآورده‌سازی نیازهای خاص هر مشتری است. نسخه‌های از پیش پیکربندی‌شده **PT AF™ برای محافظت از موارد زیر توسعه یافته‌اند:

+ بانک‌ها و موسسات مالی
+ پورتال‌های رسانه‌ای
+ شرکت‌های مخابراتی
+ سیستم‌های ERP



مدل‌های استقرار

PT AF™ مدل‌های استقرار انعطاف‌پذیری را برای تطبیق با سیاست‌های IT مورد نظر شرکت شما ارائه می‌دهد. این سیستم می‌تواند به‌عنوان **یک دستگاه مجازی(VM)، دستگاه سخت‌افزاری** یا به‌صورت **نرم‌افزار به عنوان سرویس (SaaS)** پیاده‌سازی شود. همچنین می‌توان آن را در یکی از سه حالت زیر پیکربندی کرد:

+ حالت درون‌خط (In-line Mode): ترافیک از طریق PT AF™ هدایت می‌شود که به‌طور فعال حملات را شناسایی و جلوگیری می‌کند.
+ حالت آینه (Mirror Mode): یک روتر ترافیک را به PT AF™ منعکس می‌کند که سپس تهدیدات بالقوه را شناسایی کرده و به سیستم‌های امنیتی موجود شما هشدار می‌دهد.
+ حالت خارج از خط (Off-line Mode): PT AF™ لاگ‌ها را برای شواهدی از حملات قبلی جهت تحلیل قانونی بررسی می‌کند.

قابلیت‌های اضافی

+ محافظت در برابر تمامی آسیب پذیری‌های شناخته‌شده توسط OWASP و WASC، از جمله SQLi، XSS و XXE، و همچنین حملاتی مانند تقسیم درخواست HTTP، کلیک‌دزدی (Clickjacking) و حملات پیچیده سمت کلاینت (مانند XSS مبتنی بر DOM).
+ دفاع پیشگیرانه از درخواست‌ها، داده‌ها و کوکی‌ها به شما امکان می‌دهد تا حملاتی مانند CSRF را مسدود کنید، حتی اگر توسعه دهندگان ابزارهای امنیتی موردنیاز را نادیده گرفته باشند.
+ یکپارچه‌سازی موثر با سیستم مدیریت امنیت اطلاعات شرکت: امکان یکپارچه‌سازی با آنتی ویروس‌ها، DLP، ضد DDoS و SIEM.
+ مکانیزم‌های ضد تقلب و ضد بات شامل خدمات پروفایلینگ و اعتبارسنجی که رفتار غیرعادی کاربران (مانند ورود از آدرس غیرعادی) را شناسایی می‌کند.
+ مطابقت با استانداردهای امنیتی PCI DSS و سایر استانداردهای بین‌المللی، ملی و شرکتی.
+ عملکرد بالا: PT AF™ با هدف دسترسی‌پذیری بالا طراحی شده است. این سیستم می‌تواند به صورت فعال-فعال یا فعال-غیرفعال استقرار یابد. سازمان‌ها می‌توانند از تعادل بار در هسته PT AF™ استفاده کرده یا از یک تعادل‌دهنده بار خارجی بهره‌مند شوند.
+ این قابلیت‌ها PT Application Firewall™ را به یک راهکار قدرتمند برای حفاظت از برنامه های کاربردی در برابر تهدیدات امنیتی تبدیل می‌کنند.

آیا شرکت شما تحت حمله قرار گرفته است؟

شبکه و محیط خارجی خود را بررسی کنید.برای درخواست آزمایشی رایگان PT ، با ما تماس بگیرید.

pt@magsaco.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 سریع ترین 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.

MAGSA magsaco.ir شرکت مگسا (مهندسی گسترش سامانه امن) یکی از شرکت های با سابقه و فعال در حوزه امنیت فضای تولید و تبادل اطلاعات است که در سال ۱۳۸۲ شکل گرفت و در سال ۱۳۸۴ تاسیس شد. حوزه های اصلی فعالیت این شرکت با دو رویکرد اصلی است.

رویکرد فنی امنیت که شامل امنیت نرم افزار، امنیت شبکه، امنیت اطلاعات و امنیت زیرساختهای صنعتی است. رویکرد مدیریت امنیت که شامل طراحی طرحهای جامع امنیت شبکه، طرح جامع امنیت سایبر، ارزیابی سطح بلوغ امنیت سایبری و پیاده سازی سیستم مدیریت امنیت اطلاعات است. طی دو دهه گذشته، خدمات گوناگونی در هر دو حوزه توسط شرکت به سازمانها، نهادها، شرکت ها و سایر مشتریان شرکت ارائه شده است.

درحال حاضر مگسا به عنوان شرکت توزیع کننده محصولات PT در ایران فعالیت میکند

شرکت Positive Technologies

Positive Technologies پیشرو در صنعت امنیت سایبری و ارائه‌دهنده جهانی راهکارهای امنیت اطلاعات است.

ماموریت ما: حفاظت از کسب‌وکارها و صنایع مختلف در برابر حملات سایبری و آسیب‌های غیرقابل‌تحمل.

بیش از ۳,۳۰۰ سازمان در سراسر جهان از فناوری‌ها و خدمات توسعه‌یافته توسط شرکت ما استفاده می‌کنند.

ptsecurity.com