SANGFOR NGAF

فایروال نسل بعد

امنیت هوشمند، قدرت گرفته از هوش مصنوعی

اولین فایروال نسل بعدی یکپارچه شده با WAF

- یک پنل مدیریتی واحد برای تمام عملیات امنیتی
- قابلیت تخصص امنیتی از طریق تجسم
- کار بیشتر با هزینه کمتر. حداقل 50٪ کاهش هزینه تمام شده
- کاهش رد پای وابستگی سخت افزاری تا 70%

Gartner

Magic Quadrant for Enterprise Network Firewalls

ICSA labs
CERTIFIED FIREWALL - CORPORATE

SANGFOR

دنیای جدید، فناوری جدید، امیت جدید

صنعت IT بطور مداوم در حال پیشرفت است. در حال حاضر اینترنت به سمت فناوری اطلاعات مانند رایانش ابری، BYOD و IoT در حال گسترش و بهبود است.
اینترنت با برنامه های مهم تجاری و خدمات فناوری اطلاعات بدون محدودیت های زمانی و مکانی و با تجهیزات و امکانات نامحدود در اختیار کاربران است. این روندها هر روزه در حال پیشرفت و در حال گسترش هستند و به مانند یک موجود زنده در حال رشد و تکامل است، اما آیا امنیت شبکه با همان سرعت در حال پیشرفت است؟
اخلاقیات عموما هیچگاه بیشترین نقش را در روند تکامل نداشته است و صنعت فناوری اطلاعات نیز از این قاعده مستثنی نیست. اطلاعات، جدیدترین ارز و ارزش در تجارت جهانی است و داده های حساس مانند اطلاعات مالی و اطلاعات محرمانه شرکت ها به طور قابل توجهی هدف عناصر خورنده مانند بدافزار، باج افزار و هک است.

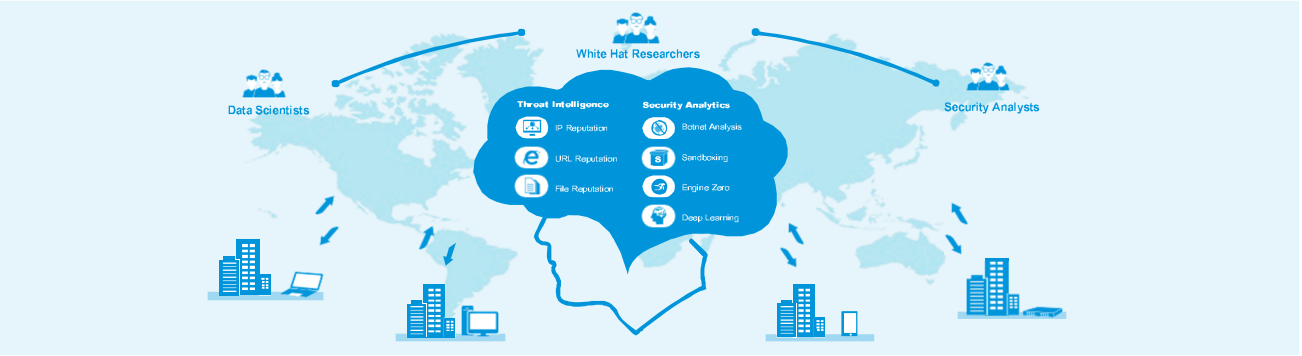
در سال 2017 ، نوع جدیدی از باج افزار به نام WannaCry بیش از 99 کشور را آلوده کرد و به دولت ها مدارس، بیمارستان ها و سایر صنایع حمله کرد. همین حادثه بود که باعث شد باج افزار به خوبی برای عموم مردم شناسایی شود. بدافزار، نرم افزاری مخرب است که مجرمان اینترنتی از آن برای نگهداری پرونده های شما (یا رایانه) برای باج استفاده می کنند و شما را مجبور به پرداخت مبلغ مشخصی می کنند تا با رمزگذاری پرونده های خود ، آنها را پس بگیرید. از زمان کشف ، باج افزار با آلوده شدن هرچه بیشتر کاربران ، اعم از شرکت ها و مصرف کنندگان ، با سرعت فوق العاده ای در حال رشد است. این امر به طور جدی بر بهره وری و شهرت و اعتبار بسیاری از شرکت ها تأثیر می گذارد ، که در پایان بسیاری از آنها مجبور به پرداخت مبالغی می شوند.
اکنون انواع مختلفی مانند XBash در حال گسترش هستند که تمرکز آنها بر تخریب سیستم داده و استخراج رمز ارز است. امنیت برنامه، دیگر اختیاری نیست. بین افزایش حملات و فشارهای نظارتی ، سازمان ها باید فرایندها و قابلیت های موثر برای امنیت برنامه ها و API های خود را ایجاد کنند) منبع OWASP :. 2017 .(با توجه به آگاهی از خطر و نگرانی های مربوط به هزینه ها ، تأخیر در ایجاد امنیت واقعی سازمانی ، بسیاری از مشاغل صرفاً بدون توجه به نیازهای واقعی (یا تصوری از) نیازهای واقعی خود را انجام می دهند.

فایروالِ برنامه ی نسل بعدی سنگفور

Sangfor NGAFیک راه حل امنیتی همگرا است که با استفاده از ویژگی های امنیتی یکپارچه مانند FW ، IPS، AV، ضد بدافزار ، APT، فیلتر کردن URL ، Cloud Sandboxو WAF در برابر IPS ، تهدید پیشرفته ، بدافزار ، ویروس ، باج افزار و حملات مبتنی بر وب محافظت می کند Sangfor NGAF .از Cloud Sandbox مخصوص خود برای جداسازی تهدیدات احتمالی که هنوز به هیچ پایگاه داده امنیتی اضافه نشده اند ، استفاده می کند ، به ویژه در برابر حملات روزه موثر است.
Neural-X ، جدیدترین نوآوری امنیتی Sangfor ، در هسته وب پیچیده ای از عناصر امنیتی شبکه توسعه یافته Sangfor مانند هوش تهدید ، یادگیری عمیق ، WAF، ZSand، Botware Malware Detectionو Engine Zero است Neural-X .به عنوان یک پلت فرم اطلاعاتی و تحلیلی مبتنی بر ابر که از هوش مصنوعی (AI) قدرت می گیرد ، قابلیت های شناسایی امنیت شبکه ، نقطه پایانی و امنیت به عنوان سرویس Sangfor را تقویت و گسترش می دهد.

دنیای هوشمند ، دنیای ایمن با نوآوری های Sangfor

Neural-X در مرکز عناصر امنیت شبکه Sangfor است. Neural-X ، به عنوان یک پلت فرم اطلاعاتی و تحلیلی مبتنی بر ابر که از هوش مصنوعی (AI)قدرت می گیرد ، قدرت تشخیص و گسترش قابلیت های شناسایی امنیت شبکه ، نقطه پایانی و خدمات امنیتی Sangfor را فراهم می کند.



Neural-X شامل ده ها مولفه بهم پیوسته است که برای کار یکپارچه باهم طراحی شده اند تا سیستم شما را امن نگه دارند ، از جمله صفر موتور ، هوش تهدید ، یادگیری عمیق ، جعبه شن و تشخیص بات نت.

یادگیری عمیق

یادگیری عمیق یک عنصر پیچیده از یادگیری ماشین است که از عملکرد اتصال نورونها در مغز انسان الهام گرفته شده است. این بخشی از هوش مصنوعی است و می تواند به عنوان یک تکامل برای یادگیری ماشین در نظر گرفته شود. همانطور که از نام آنها بر می آید ، می تواند به خودی خود با پردازش میلیون ها داده ، بیاموزد تا بتواند دقیق تر و سریعتر پیش بینی کند.

یکی از راه هایی که Neural-X از یادگیری عمیق استفاده می کند ، تجزیه نام دامنه های رمز آلود به بردارهایی است که قابل خواندن در ماشین هستند. تجزیه و تحلیل عمیق وابستگی برداری، نام دامنه های مورد استفاده توسط بدافزارهای خانواده های مشابه را تشخیص می دهد. با گذشت زمان ، عملکرد یادگیری عمیق به طور مستقل شروع به کار و یادگیری می کند - بنابراین یک رویکرد فعال در مورد بدافزار را حفظ می کند.

ردیابی بات نت

هکرها با کنار گذاشتن آدرس های IP ثابت پیچیده تر می شوند و به جای آن از نام دامنه های پویا استفاده می کنند. این نام های دامنه رمزنگاری برای اتصال botnet به کنترل کننده آنها با استفاده از الگوریتم های مخفی استفاده می شود. تشخیص آنها بسیار دشوار است زیرا نمایش داده های DNS ، رفتاری مشابه با یک کاربر متوسط دارند Neural-X . برای کشف بات نت ها از تجزیه و تحلیل جریان پیشرفته ، محاسبه بصری و فناوری یادگیری عمیق استفاده می کند. این سیستم قادر است نام دامنه های مخرب بیشتری را در مقایسه با منابع معروف مانند VirusTotal کشف کند. تاکنون بیش از یک میلیون نام دامنه مخرب کشف کرده است و این لیست روزانه در حال رشد است.

نسل بعدی فایروال برنامه وب

موتور WAF نسل بعدی که در فایروال نسل بعدی Sangfor تلفیق شده است ، برای محافظت در برابر حملات جدید مبتنی بر وب مانند تزریق SQL ، پوسته های وب ، تزریق struts2و عیب زدایی تولید شده است. موتور NGWAF Sangfor از یادگیری ماشینی و عمیق برای تجزیه و تحلیل رفتارهای حمله استفاده می کند. این میزان تشخیص را افزایش می دهد و باعث کاهش مثبت کاذب از موتورهای سنتی مبتنی بر SNORT می شود. با مدل سازی رفتارهای حمله ، یک مدل تهدید ایجاد می شود تا تهدیدات سیستم برنامه ها را به راحتی مدیریت کند.

موتور صفر

Engine Zero یک موتور اصلی شناسایی بدافزار است که بر اساس مجموعه ای از فناوریهای قدرتمند هوش مصنوعی ساخته شده و توسط تیمی از دانشمندان داده ، تحلیلگران امنیتی و محققان کلاه سفید تقویت شده است. این موتور یکی از موتورهای بازرسی بدافزار است که در راه حل های امنیتی شبکه Sangfor ، راه حل نقطه پایانی و پلت فرم ابر Neural-X تعبیه شده است. بسیار کارآمد است و از منابع بسیار کمی استفاده می کند. فقط چنین کارآیی می تواند بدافزار را برای حملات شناخته شده و صفر روزه به دروازه شبکه فراهم کند که تقریباً هیچ تاثیری بر عملکرد ندارد. در آزمایشات اخیر (ژوئیه 2018) ، میزان تشخیص بدافزار ما از نظر دقت و پیشی گرفتن از سایر فروشندگان و گزینه های منبع باز ، بالاترین امتیاز را دارد.

هوش تهدید

Neural-X هسته اصلی شناسایی و دفاع در برابر تهدیدات هوشمند است. در هوش تهدید، اطلاعات سازمان یافته ، تجزیه و تحلیل و تصفیه شده است که به سازمان ها امکان می دهد خطرات شناخته شده و شدید ناشی از منابع خارجی را درک ، ارزیابی و از بروز آنها جلوگیری کنند.

ZSand

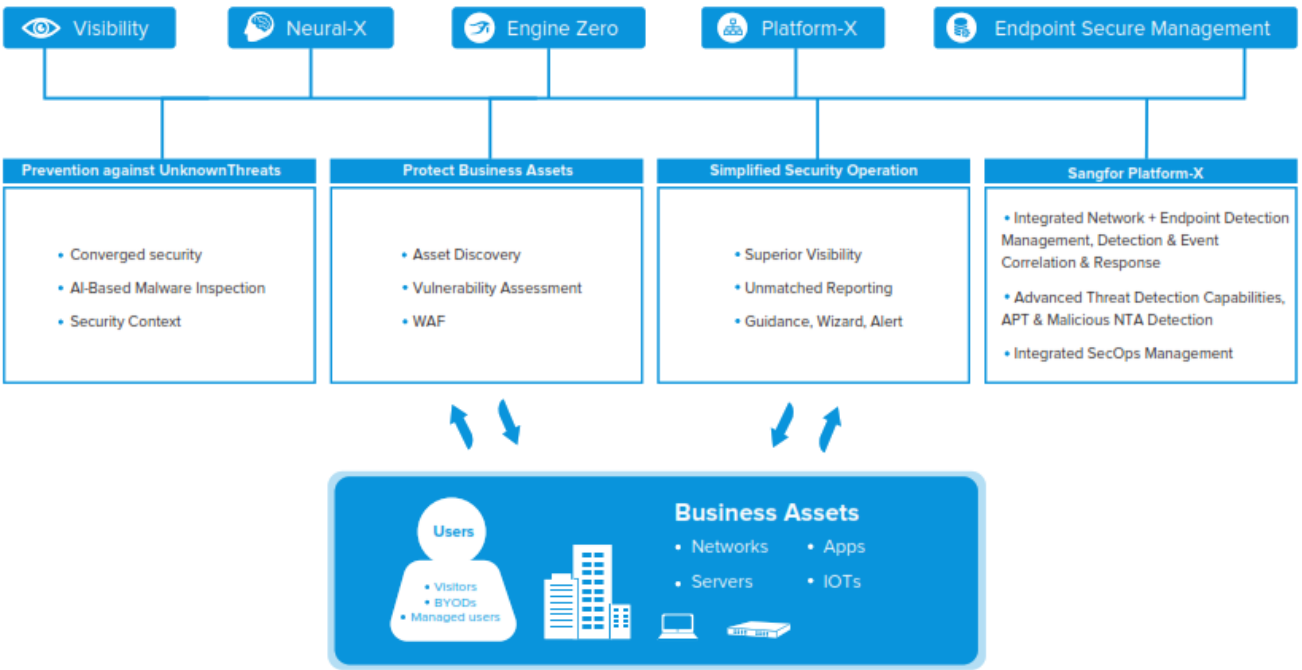
Sangfor ZSandیک فناوری اجرای پویا مجازی (sandboxing)است که برای شناسایی بدافزار ناشناخته طراحی شده است Sangfor ZSand .بدافزار مشکوک را در یک محیط امن و کنترل شده اجرا می کند و رفتارهای غیر طبیعی این پرونده ها را برای شناسایی و پیشگیری در آینده نظارت می کند. ZSand در آزمایشات اخیر ، خانواده های باج افزار از جمله GandCrab، Zusy، GlobeImposterو LockCryptرا به دقت شناسایی کرده است . تمام داده ها را با هوش تهدیدات Neural Xبه اشتراک می گذارد و امکان شناسایی و مطالعه بدافزار را بدون هیچگونه امضای قبلی مشخص می کند و خطر حملات روز صفر در آینده را کاهش می دهد.

مفهوم Sangfor از امنیت

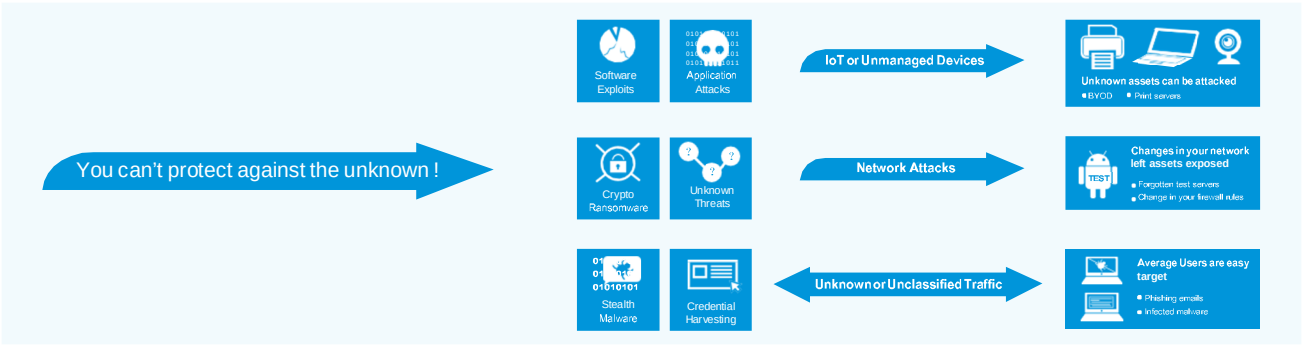
.

Sangfor Technologiesمفهوم جدیدی از امنیت شبکه برای مقابله با تهدیدات جدید و خطرناک تر دارد. ما بیشتر پیش می رویم تا یک راه حل محافظت کامل برای همه کاربران در برابر تهدیدات داخلی یا خارجی ، موجود یا آینده ارائه دهیم. سازگاری تکاملی Sangfor از امنیت شبکه 4 نکته اساسی را دنبال می کند که هسته اصلی استراتژی بازار ما را تشکیل می دهند.

امنیت شبکه در همه موارد عمودی تکامل یکسانی را تجربه نکرده است - کارشناسان امنیتی در بخشهای مختلف و مکانهای مختلف نظرات ، انتظارات و نیازهای مختلفی دارند. در حالی که برخی امنیت شبکه را به عنوان محافظت در برابر دسترسی غیر مجاز به پرونده ها و داده ها تعریف می کنند ، برخی دیگر بر فایروال ، آنتی ویروس و ردیابی بات نت تمرکز دارند. راه حل های امنیتی سنتی دارای دید محدودی از کاربران ، ترافیک و دارایی های فناوری اطلاعات بدون قابلیت شناسایی در زمان واقعی یا پس از رویداد هستند. با افزایش حملات به لایه برنامه ، امنیت شبکه نیاز به تکامل بیشتری دارد تا با تهدیدات ظاهر شود.



پیشگیری در برابر تهدیدهای ناشناخته



Sangfor NGAF یک راه حل امنیتی همگرا است ، که در برابر تهدیدات مداوم پیشرفته (APT) ، بدافزار (ویروس ، باج افزار) و حملات تحت وب محافظت می کند . Sangfor NGAFدارای ویژگی های امنیتی کاملی مانند فایروال ، سیستم جلوگیری از نفوذ (IPS) ، ضد ویروس (AV) ، موتور ضد بدافزار ، حفاظت APT (تهدیدهای ممتد پیشرفته) ، فیلتر کردن URL ، جعبه ایمنی Cloud و فایروال برنامه وب است.

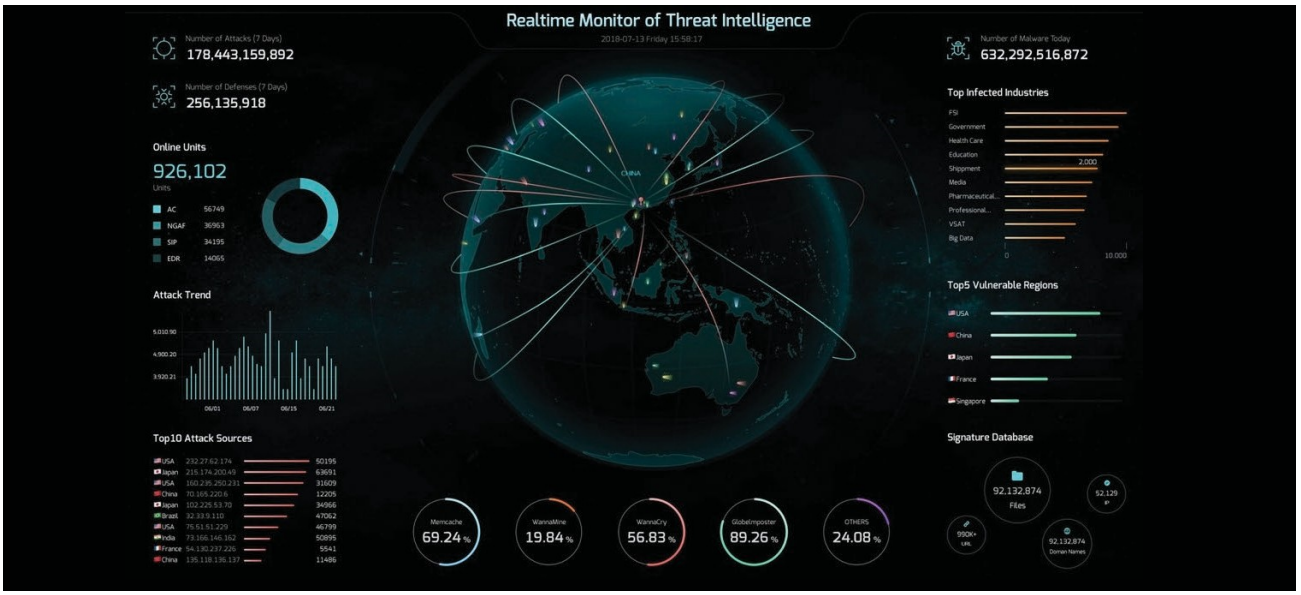
Sangfor NGAF از Cloud Sandbox مخصوص خود برای کمک به کاربران در جداسازی تهدیدات بالقوه در حال ظهور و جدید که در هیچ پایگاه داده امنیتی وجود نداشته است استفاده می کند ، که به ویژه در برابر حملات روز صفر مفید است.

عنصر انسانی هنوز یکی از ضعیف ترین عناصر در تیم عملیاتی امنیت سازمان است. با هزاران لاگ، عبور از هر یک از آنها تقریباً غیرممکن است. به همین دلیل بسیاری از NGFW تمام لاگ (عبور)های مربوط را فیلتر می کنند و فقط موارد دارای بالاترین سطح اهمیت را نشان می دهند. با این حال حتی با این وجود ، هنوز هم می توان خطا کرد.

به همین دلیل است که Sangfor اکنون پیشرفت بیشتری کرده و هوش مصنوعی را در تمام نوآوری های امنیتی خود مانند شناسایی بدافزار "Engine Zero" ، نسل بعدی WAF و موتورهای جدید Botnet ردیابی کرده است.

همه این موتورها از هوش تهدیدی یکسانی برخوردار هستند که توسط پلت فرم Neural-X مبتنی بر ابر سنگفور ارائه شده است. با استفاده از یادگیری ماشینی ، می تواند تهدید ناشناخته جدید را بدون هیچ گونه امضای موجود از قبل تشخیص دهد و از آسیب های سازمان شما جلوگیری کند.

نظارت بر زمان واقعی هوش تهدید



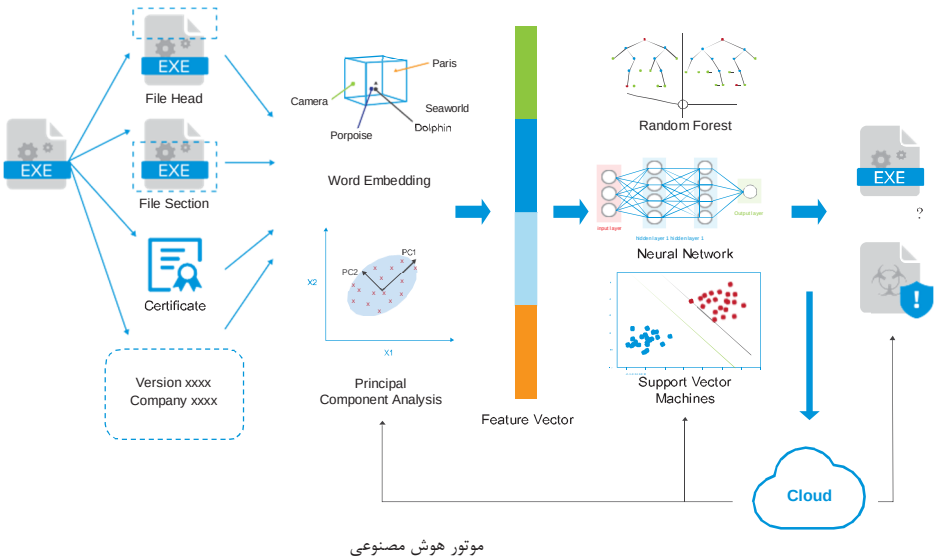
منابع هوش

- بیش از 20،000 دروازه شبکه متصل IOC را ارائه می دهند که شامل URL های مخرب ، IP ، نام دامنه ها و هش های بدافزار با تعداد دروازه های شرکت کننده در هر سال دو برابر می شود.
- خوراک هوش تهدید شخص ثالث
- تحقیق و توسعه امنیتی **Sangfor** به دو جامعه کلاه سفید و کلاه سیاه

سناریوی مورد واقعی

اگر Sangfor NGAF اتصال غیرمعمولی خروجی را در سرور متصل به اینترنت تشخیص دهد ، آدرس مشکوک DNS را برای تأیید به Neural-X ارسال می کند. اگر هوش تهدید این DNS خاص را به عنوان یک سرور شناخته شده C&C طبقه بندی کرده باشد ، به احتمال زیاد سرور به خطر افتاده است .NGAF می تواند به گونه ای برنامه ریزی شود که این ارتباطات C&C را مسدود کند بنابراین دیگر خسارتی ایجاد نخواهد شد و همچنین برای بررسی و پردازش بیشتر هشدارهایی برای اپراتورهای فایروال ارسال می شود.

موتور ردیابی قدرت گرفته از هوش مصنوعی



موتور هوش مصنوعی

موتور صفر در مقایسه با فن آوری های تشخیص سنتی

فن آوری های سنتی تشخیص عمدتا شامل MD5 ، امضای ویروس ، تطبیق قوانین ، اجرای مجازی و سندباکس است. از لحاظ تئوری ، با کاهش عملکرد و افزایش هزینه ، توانایی تشخیص آنها از MD5 به جعبه ماسه قویتر می شود. در مقایسه با این فن آوری های سنتی ، موتور صفر دارای مزایای زیر است:

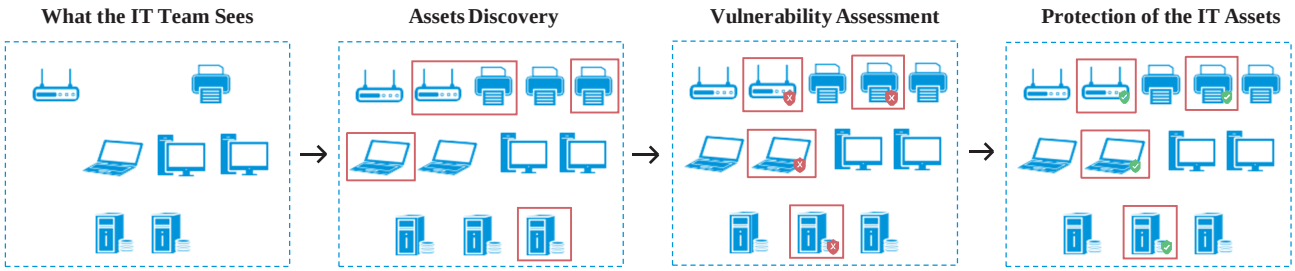
- توانایی تعمیم قوی برای شناسایی ویروس های ناشناخته یا انواع جدید. به لطف توانایی تعمیم یادگیری ماشین ، موتور صفر می تواند ویروس های ناشناخته یا انواع جدید ویروس های شناخته شده را بدون نیاز به دیدن نمونه ها شناسایی کند. با این حال ، راه حل های سنتی ابتدا باید نمونه بگیرند ، که این امر می تواند باعث تاخیر شود. توضیح دقیق این موضوع را می توان در بخش 2,2,1 یافت..
- سرعت سریع. سرعت اسکن نزدیک به خط نزدیک به MD5.
- اشتغال کم حافظه. از نظر هزینه منابع، موتور صفر فقط کمتر از 200 مگابایت حافظه را اشغال می کند ، که کوچکتر از موتورهای سنتی شناخته شده است.
- درجه بالایی از اتوماسیون. مدل Engine Zero بدون دخالت انسان می تواند به طور خودکار ویژگی ها را یاد بگیرد و استخراج کند. مدل در ابر تکامل یافته ، با توانایی تشخیص و درجه اتوماسیون بهبود یافته است. با این حال ، فن آوری های تشخیص سنتی به متخصصان ویروس نیاز دارند که به صورت دستی اثر انگشت و امضاهای ویروس را استخراج کنند ، که نه تنها هزینه بر است بلکه عقب مانده است. از آنجا که فروشندگان سنتی ضد ویروس می توانند پایگاه داده ویروس را به روز کنند ، ممکن است باعث باقی ماندن ویروس برای مدت طولانی شود.

راه حل های تشخیص سنتی ناکافی نیز دارای ارزش منحصر به فردی هستند. به عنوان مثال ، آنها می توانند سریعتر به مکانیسم لیست سیاه و سفید پاسخ دهند. بنابراین ، با طراحی موتور صفر برخی از فن آوری های سنتی نیز به کار می رود تا یک راه حل مخرب برای شناسایی پرونده ها بر اساس هوش مصنوعی و فن آوری های سنتی تشکیل دهد.

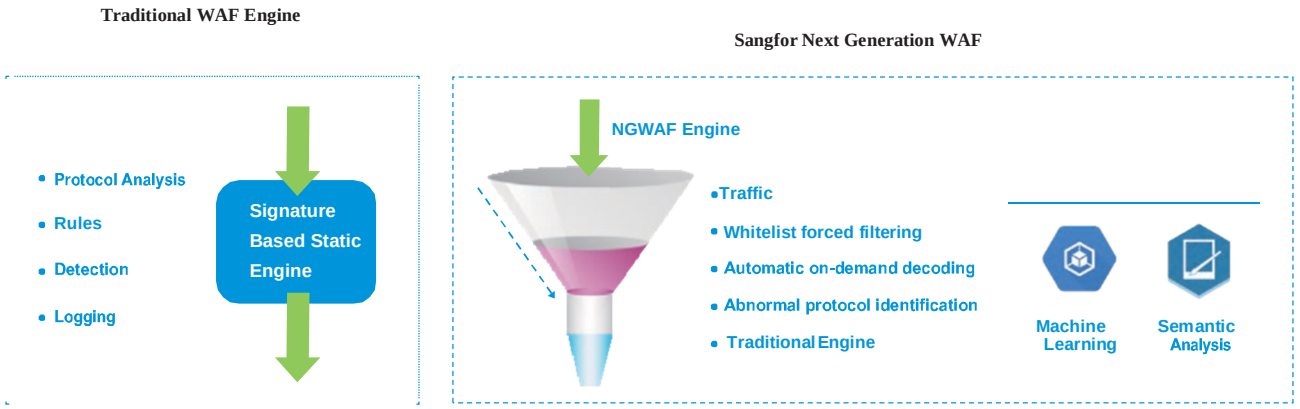
حفاظت از دارایی های تجاری

Sangfor NGAF در کشف و محافظت از دارایی های تجاری تبحر دارد Sangfor NGAF .می تواند به طور خودکار مجموعه اطلاعات سازمان شما را کشف کند ،آسیب پذیری های سیستم را در زمان واقعی بیابد و به طور مداوم از دارایی های فناوری اطلاعات محافظت کند.

علاوه بر این Sangfor NGAF با محافظت پیشگیرانه خود قادر به اعمال وصله های مجازی ، شناسایی رمزهای عبور ضعیف و برنامه های پنهان در کلیه دارایی های IT است.



با موتور WAF نسل بعدی خود که از یادگیری و تجزیه و تحلیل معنایی استفاده می کند ، به محافظت در برابر شایع ترین حملات مانند پوسته شبکه ، تزریق struts2 و عیب یابی کمک می کند. همچنین می تواند تجزیه و تحلیل حملات و رفتارهای حمله را بیاموزد. این امر میزان تشخیص را افزایش می دهد و مثبت کاذب موتور سنتی مبتنی بر SNORT را کاهش می دهد. با مدل سازی رفتارهای حمله ، مدل تهدید برای مشتریان ایجاد می شود تا بتوانند تهدیدات سیستم برنامه را به راحتی مدیریت کنند.



- برای شناسایی تهدیدات ناشناخته و آسیب پذیری های پر خطر به طور جامع از قوانین طبقه بندی پیشی می گیرد
- به طور خودکار با مدلسازی ترافیک عادی کسب و کار ، مثبت کاذب تا حد 62,4% کاهش می یابد

- شناسایی تهدیدات و سو استفاده های ناشناخته امکان پذیر نیست
- امکان دور زدن آن
- مثبت کاذب درتشخیص تزریق SQL
- - عملکرد سطح پایین

عملیات امنیتی ساده شده

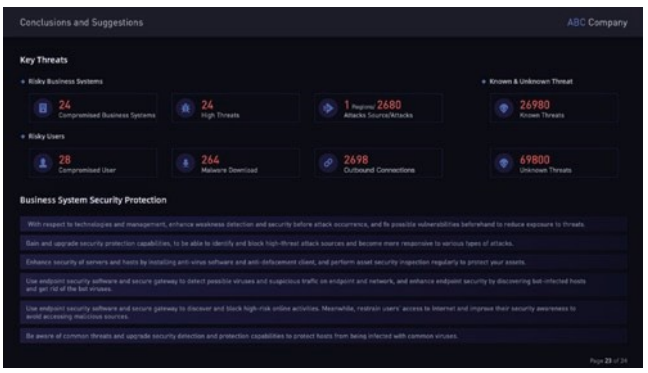
حتی سازمانهای کوچک یا متوسط بدون تیم امنیتی تخصصی فناوری اطلاعات اغلب هزاران هشدار در هفته دریافت می کنند که به بخش فناوری اطلاعات نیاز دارد تا نفر-ساعت زیادی را به تحقیق و تجزیه و تحلیل اختصاص دهد و هزینه های عملیاتی را افزایش دهد. کابوس IT تازه آغاز شده است ، زیرا اکنون مسئولیت محدود کردن زمان خرابی ، شناسایی علت اصلی و اقدام برای کاهش خسارات و جلوگیری از حمله در آینده از همان منبع را دارند. این سازمان ها هنوز از راه حل های امنیتی سنتی و فاقد هرگونه ابزار جستجوی هوشمند یا خودکار که در معرض آسیب جدی هستند، استفاده می کنند. بدون دید 360 درجه و تجزیه و تحلیل و گزارش های واضح ، امنیت موثر از نظر نمایی دشوارتر می شود.

Sangfor NGAFبا استقرار آسان و بهره برداری ساده و ویژگی های نگهداری ، امنیت قابل اعتماد و بی دردسری را فراهم می کند ،باعث ایجاد یک محیط IT موثر و ایمن می شود. ویزارد پیکربندی NGAF گسترش سیاست های امنیتی را ساده می کند در حالی که ابزارهای جستجوی بصری یکپارچه ، امنیت کلی یک سازمان را از سیستم های تجاری تا نقاط نهایی به انجام می رساند.

Sangfor NGAF با کمک به شناسایی وقایع امنیتی واقعی و پر خطر در میان هزاران هشدار و ارائه راهنمایی و پیشنهادات برای بهترین راه حل ، اقدامات امنیتی روزمره را ساده می کند.

گزارش اجرایی برای تیم مدیریت

عملیات ساده روزانه



بررسی اجمالی امنیت کاربر

نتیجه گیری و پیشنهادات

قابلیت مشاهده (درک) امنیت

با درهم آمیختن ترافیک مخرب و ترافیک قانونی بحث امنیت پیچیده تر می شود و کاربران مجاز در معرض خطر حمله (آگاهانه یا ناآگاهانه) بوده و یک خطر بالقوه برای شبکه هستند Sangfor .معتقد است که نمایان بودن کل شبکه پایه و اساس مدیریت شبکه جامع است. مدیران باید تمام خطرات موجود در دارایی های اطلاعات را به وضوح ببینند و درک کنند و کاربران و رفتارها را ردیابی کنند تا تهدیدات امنیتی را شناسایی کرده و به موقع آنها را برطرف کنند. داده ها و آمار مربوط به تهدیدات گذشته و فعلی بسیار حیاتی است ، اما همچنین نیاز به تجزیه و تحلیل بیشتر در مورد ارتباط بین کاربران ، رفتارها و سیستم های تجاری وجود دارد. با تکامل امنیت به نمای 360 درجه از شبکه ، کاربران می توانند درک بهتری از منشأ حمله ، روند حمله ، جبران هرگونه آسیب و دفاع پیشگیرانه در برابر حملات بعدی بدست آورند.

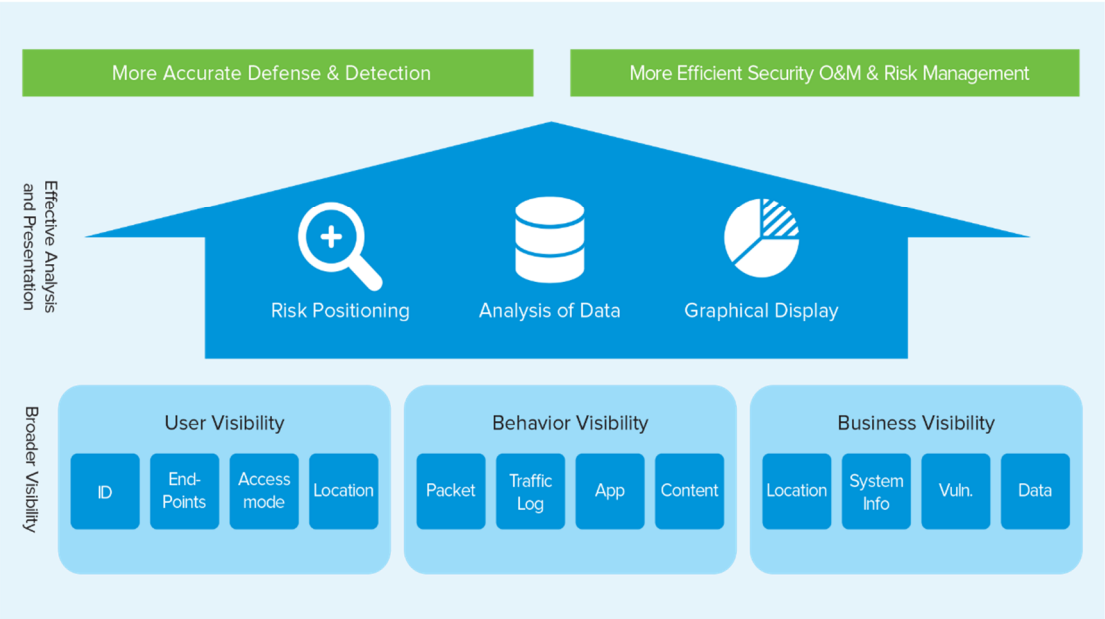
ابزارهای گزارشگری Sangfor NGAF به مشتریان ما تنها با چند کلیک نمای کلی از شبکه خود را ارائه می دهد. اطلاعاتی مانند هویت کاربر آنلاین ، سرور یا ترافیک غیرعادی و وضعیت حمله و منبع تنها برخی از منابع دید ارائه شده است.

تجزیه و تحلیل و ارائه موثر : موقعیت یابی ریسک | تجزیه و تحلیل داده ها | نمایش گرافیکی

قابلیت مشاهده بیشتر : کاربر | رفتار | تجارت | تهدیدها | خطرات | رویدادهای امنیتی

Neural-X در هسته شناسایی و دفاع تهدیدات هوشمند NGAF قرار دارد. Neural-X با استفاده از یادگیری عمیق و تجزیه و تحلیل عمیق ارتباط بردار برای شناسایی نام دامنه های مورد استفاده توسط بدافزارهای خانواده های مشابه استفاده می کند. عملکرد یادگیری عمیق برای عملکرد و یادگیری مستقل طراحی شده تا یک رویکرد فعال ، ابتکاری و بسیار قابل مشاهده برای کشف ، شناسایی و حذف بدافزار را حفظ کند.

هوشمندی، کلید اصلی سنگفور برای مشاهده است و هدف Sangfor NGAF و Neural-X ارائه یک نمای کلی از شبکه با قابلیت مشاهده جامع از نقاط انتهایی تا سیستم های تجاری است.



Sangfor Platform-X

Sangfor Platform-X یک پلت فرم مدیریت امنیتی مبتنی بر ابر است که برای مدیریت کلیه محصولات امنیتی Sangfor در فضای ابری با جمع آوری ، تجزیه و تحلیل و نمایش همه گزارش های امنیتی مجهز شده است. از طریق ادغام با راه حل امنیتی مبتنی بر ابر Sangfor ، Neural-X ، Platform-X با هشدار به مدیران در مورد حملات یا تهدیدها در زمان واقعی ، امنیت و شناسایی جامع را امکان پذیر می کند ، بنابراین عملیات امنیتی را بسیار ساده می کند.

امنیت متمرکز قابل مشاهده

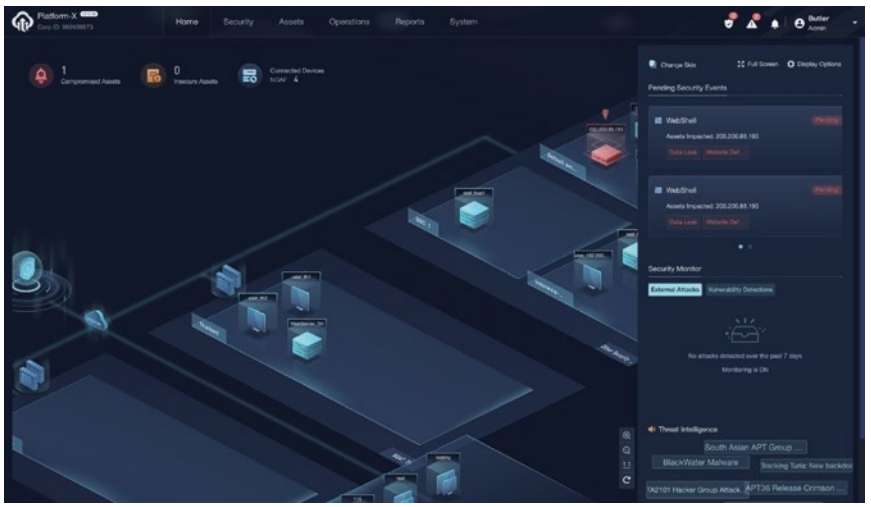
Platform-X مجموعه لاگ دستگاه های امنیتی را یکپارچه می کند، تجزیه و تحلیل را ارائه می دهد و نتایج را نمایش می دهد. علاوه بر این ، نظارت بر حادثه امنیتی مبتنی بر توپولوژی ، ارزیابی و گزارش وضعیت امنیتی ، تشخیص و پردازش همبستگی بین دستگاه های امنیتی را فراهم می کند.

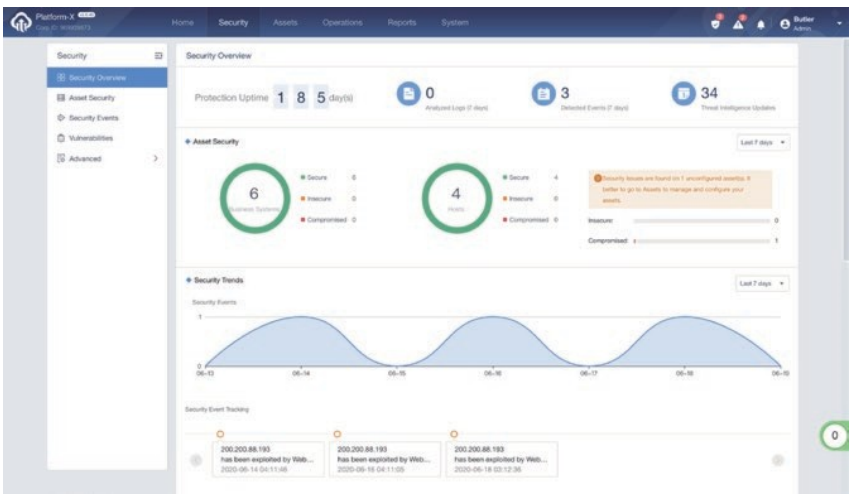
هوش تهدید مشترک

همکاری عمیق تجزیه و تحلیل داده های بزرگ ، تحلیلگران امنیتی و محققان کلاه سفید ، Platform-X را مجهز کرده است تا حملات پیشرفته و رفتار تهدیدآمیز بالقوه را شناسایی کند و شاخص های مهمی را برای تحقیق و شناسایی تهدید فراهم کند.

مدیریت دستگاه واحد

Platform-X مانیتورینگ یکپارچه وضعیت سخت افزار ، ارتقاء سیستم عامل ، همگام سازی سیاست ها و ورود از راه دور و بدون رمز عبور را فراهم می کند.





SANGFOR NGAF Product Family

Model	AF-1000-B1080*	AF-1000-B1120*	M4500-F-I	M5100-F-I	M5150-F-I	M5200-F-I	M5250-F-I	M5300-F-I	M5400-F-I
Profile	Desktop	1U	Desktop	1U	1U	1U	1U	1U	1U
RAM	2G	2G	4G	4G	4G	4G	4G	8G	8G
HD Capacity	SSD 64GB	SSD 64GB	SSD 64GB	SSD 64GB	SSD 64GB	SSD 64GB	SSD 64GB	SSD 64 GB	SSD 128 GB
Firewall Throughput[1]	1.05 Gbps	1.75 Gbps	2 Gbps	2.8 Gbps	3.5 Gbps	4.9 Gbps	5.5 Gbps	12 Gbps	20 Gbps
NGFW Throughput[2]	800 Mbps	1 Gbps	1.4 Gbps	2.5 Gbps	2.5 Gbps	2.8 Gbps	2.8 Gbps	5 Gbps	8.4 Gbps
IPS + WAF Throughput (HTTP)	N/A	700 Mbps	1.2 Gbps	1.4 Gbps	1.4 Gbps	2.1 Gbps	2.1 Gbps	3.85 Gbps	5.6 Gbps
Threat Protection[3] Throughput	600 Mbps	800 Mbps	1 Gbps	1.8 Gbps	1.8 Gbps	2.1 Gbps	2.1 Gbps	4.2 Gbps	5.6 Gbps
IPsec VPN Throughput	100 Mbps	100 Mbps	250 Mbps	250 Mbps	250 Mbps	375 Mbps	375 Mbps	1 Gbps	1.25 Gbps
Max IPsec VPN Tunnels	100	100	300	300	300	500	500	1000	1500
Concurrent Connections (TCP)	800,000	800,000	250,000	750,000	1,000,000	1,200,000	1,800,000	2,000,000	2,500,000
New Connections (TCP)	15,000	18,000	10,000	20,000	25,000	30,000	50,000	80,000	110,000

[1] 1518 Bytes UDP Packets.
[2] NGFW is measured with Firewall, Bandwidth Management, IPS, Application Control.
[3] Threat Prevention is measured with Firewall, Bandwidth Management IPS, Application Control, Anti Virus.

Power and Hardware Specifications

Model	AF-1000-B1080*	AF-1000-B1120*	M4500-F-I	M5100-F-I	M5150-F-I	M5200-F-I	M5250-F-I	M5300-F-I	M5400-F-I
Support Dual Power Supplies	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Power [Watt] (Max)	60W	40W	60W	60W	40W	40W	40W	60W	150W
Temperature	0~45°C								
System Weight	1.5Kg	3.85Kg	2.0Kg	3.85Kg	3.85Kg	3.85Kg	4.24Kg	4.5Kg	6.1Kg
System Dimensions (mm³)	175 x 275 x 45	300 x 430 x 45	175 x 275 x 45	300 x 430 x 45	300 x 430 x 45	300 x 430 x 45	300 x 430 x 45	300 x 430 x 45	400 x 430 x 45
Relative Humidity	5%~95% non-condensing								
Compliance & Certificates	CE, FCC								

Network Interfaces

Model	AF-1000-B1080*	AF-1000-B1120*	M4500-F-I	M5100-F-I	M5150-F-I	M5200-F-I	M5250-F-I	M5300-F-I	M5400-F-I
Bypass (Copper)	N/A	1 pair	N/A	1 pair	1 pair	1 pair	2 pairs	1 pair	3 pairs
10/100/1000 Base-T	3	6	4	4	6	6	6	6	6
1G Fiber SFP	N/A	N/A	N/A	N/A	N/A	N/A	2	2	N/A
10G Fiber SFP+	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	2
Serial Port	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1
USB Port	2	2	2	2	2	2	2	2	2
Network Modules	N/A	N/A	N/A	N/A	N/A	N/A	N/A	1	2

1. "Optional Interface & 10G Fiber SFP" allows upgrading interfaces according to your requirement.
2. M5100-F-I are available with 6 interfaces platforms with corresponding cost.
3. All performance values are "up to" and vary depending on the system configuration.
*Only available for specific regions. Please contact us for more information.
4. 1 x network module can be customized to add one more NIC: 4x GE RJ45 | 4x GE SFP | 8x GE RJ45 | 8x GE SFP | 4x GE RJ45 & 4x GE SFP | 2x 10GE SFP+.

SANGFOR NGAF Product Family

Model	M5500-F-I	M5600-F-I	M5800-F-I	M5900-F-I	M6000-F-I	AF-2000-B3100*	AF-2000-B3200*	AF-2000-B3300*
Profile	2U	2U	2U	2U	2U	2U	2U	2U
RAM	8G	16G	16G	24G	32G	96G	128G	192G
HD Capacity	1T + 64G MSATA	1T + 64G MSATA	1T + 64G MSATA	1 TB +4G CF	1 TB +4G CF	1T+SSD 64GB	1T+SSD 64GB	1T+SSD 64GB
Firewall Throughput [1]	25 Gbps	50 Gbps	67 Gbps	105 Gbps	140 Gbps	140 Gbps	180 Gbps	240 Gbps
NGFW Throughput [2]	12.6 Gbps	23 Gbps	31 Gbps	56 Gbps	84 Gbps	90 Gbps	120 Gbps	140 Gbps
IPS + WAF Throughput (HTTP)	8.4 Gbps	14 Gbps	21 Gbps	42 Gbps	56 Gbps	63 Gbps	84 Gbps	126 Gbps
Threat Protection [3] Throughput	9.1 Gbps	18 Gbps	26.5 Gbps	50.4 Gbps	67.2 Gbps	79.4 Gbps	91.2 Gbps	105 Gbps
IPsec VPN Throughput	2 Gbps	3 Gbps	3.75 Gbps	5 Gbps	5 Gbps	7 Gbps	10 Gbps	15 Gbps
Max IPsec VPN Tunnels	3,000	4,000	5,000	10,000	10,000	15,000	20,000	30,000
Concurrent Connections (TCP)	3,000,000	4,000,000	8,000,000	12,000,000	16,000,000	20,000,000	32,000,000	35,000,000
New Connections (TCP)	220,000	300,000	330,000	450,000	600,000	650,000	800,000	900,000

[1] 1518 Bytes UDP Packets.
[2] NGFW is measured with Firewall, Bandwidth Management, IPS, Application Control.
[3] Threat Prevention is measured with Firewall, Bandwidth Management IPS, Application Control, Anti Virus.

Power and Hardware Specifications

Model	M5500-F-I	M5600-F-I	M5800-F-I	M5900-F-I	M6000-F-I	AF-2000-B3100*	AF-2000-B3200*	AF-2000-B3300*
Support Dual Power Supplies	√	√	√	√	√	√	√	√
Power [Watt] (Max)	150W	150W	150W	500W	500W	860W	860W	860W
Temperature	0~45°C							
System Weight	12.95Kg	12.95Kg	12.95Kg	20.0Kg	20.0Kg	24Kg	24Kg	24Kg
System Dimensions (mm³)	440 x 600 x 90	440 x 600 x 90	440 x 600 x 90	440 x 600 x 90	440 x 600 x 90	440 x 600 x 90	440 x 600 x 90	440 x 600 x 90
Relative Humidity	5%~95% non-condensing							
Compliance & Certificates	CE, FCC							

Network Interfaces

Model	M5500-F-I	M5600-F-I	M5800-F-I	M5900-F-I	M6000-F-I	AF-2000-B3100*	AF-2000-B3200*	AF-2000-B3300*
Bypass (Copper)	3 pairs	3 pairs	3 pairs	2 pairs	4 pairs	2 pairs	2 pairs	4 pairs
10/100/1000 Base-T	6	6	10	4	8	4	4	8
1G Fiber SFP	4	4	4	4	8	4	8	8
10G Fiber SFP+	2	2	2	2	4	8	8	8
Serial Port	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1	RJ45×1
USB Port	2	2	1	2	2	2	2	2
Network Modules	1	1	1	5	4	2	2	2

1. M5100-F-I are available with 6 interfaces platforms with corresponding cost.
2. All performance values are "up to" and vary depending on the system configuration.
*Only available for specific regions. Please contact us for more information.
3. 1 x network module can be customized to add one more NIC: 4x GE RJ45 | 4x GE SFP | 8x GE RJ45 | 8x GE SFP | 4x GE RJ45 & 4x GE SFP | 2x 10GE SFP+.

vNGAF
SANGFOR Virtual NGAF (HCI PLATFORM)

Model	vAF100	vAF200	vAF400	vAF800	vAF1600
NGFW / WAF Throughput	200 Mbps	400 Mbps	800 Mbps	1600 Mbps	3200 Mbps
Concurrent Connection (TCP)	500,000	1,000,000	2,000,000	4,000,000	4,000,000
New Connections (TCP)	10,000	20,000	50,000	80,000	80,000

System Requirements

System Requirements	vAF100	vAF200	vAF400
Virtualization Platform	SANGFOR HCI	SANGFOR HCI	SANGFOR HCI
CPU	Min. 1-Core Processor	Min. 2-Core Processor	Min. 4-Core Processor
Memory	2GB	4GB	8GB
Disk Space	32GB	32GB	32GB

System Requirements	vAF800	vAF1600
Virtualization Platform	SANGFOR HCI	SANGFOR HCI
CPU	Min. 8-Core Processor	Min. 8-Core Processor
Memory	16GB	16GB
Disk Space	32GB	32GB

SANGFOR NGAF Product Features

Firewall

- **Networking**
  - Policy routing, static routing, RIP v1/2, OSPF, BGP, and GRE.
  - Application policy-based forwarding, NAT (1-1 NAT, many-to-one NAT, NAT46, NAT64, and many-to-few NAT), VLAN tagging
  - IPv6 & IPv4 supported
  - Support multi cast traffic, SNMP v3, and Syslog server with UTF-8 format
  - Intelligent Dos/ DDos prevention
  - ARP spoofing prevention
  - HA fail-over time less than 1 second
  - Support at least 10000 security policies
  - Policies basis with "first come first match"
  - Provide management via SSH, HTTPS, CLI, and Web-based GUI
- **SSL VPN**
- **IPsec VPN**
  - IPSec Protocol: AH, ESP
  - D-H Group: MODP768 Group(1), MODP1024 Group(2), MODP1536 Group(5)
  - IPSec Authentication Algorithm: MD5, SHA-1. SHA-2
  - IPSec Encryption Algorithm: DES, 3DES, AES-192, AES-256. SANGFOR_DES
  - Auto VPN, support creating and manage VPN connection from Central Management Console Support SDWAN path selection policy
- **SD-WAN**
  - Intelligent Routing: Specific application routing, support routing based on remaining bandwidth, and best quality routing based on QOE detection
  - Dynamic Routing: RIP, OSPF, BGP
  - Tunnel Failover: Supports failure second-level switchover
  - Easy to deploy with step by step email instructions
  - Visualization of equipment operating status and geographic location distribution
  - Visualization of VPN link status and delay
  - Configuration batch management-support
  - Support for GRE
  - Support access to the centralized management platform (Central Manager), for unification management of branch appliances
  - Support for SD-WAN networking solution, rapid deployment of VPN through Sangfor Central Manager
  - Support for IPv6 services to meet the needs of user networks with IPv6 requirements

Threats Prevention

- **Full SSL inspection**
  - SSL inspection to all security modules including IPS, WAF, ATP, Access control, etc.
- **Cross-module intelligent correction**
  - Policy association of IPS, WAF and APT prevention modules.
  - Cross-module visibility reporting analysis
- **Threats prevention**
  - APT (Advanced Persistent Threat), Remote Access Trojan, Botnet, malware detection
  - Cloud-based Sandbox threats analysis
  - AI based malware detection engine, covering threats type of Trojan, AdWare, Malware, Spy, Backdoor, Worm, Exploit, Hacktool, Virus, etc.
  - Use cloud intelligence to prevent unknown and advanced threat.
- **Anti-virus**
  - Scan and kill viruses infecting HTTP, FTP, SMTP and POP3 traffic as well as viruses infecting compressed data packets
  - Support remove virus from detected malicious files
- **Email security**
  - Categorize and filter various forms of malicious emails.
  - Support detection deep into email body and attachments.
  - Support place warning messages into email title to avoid users from opening malicious emails

IPS

- **IPS signature database**
  - Prevention against vulnerability exploits towards various system, application, middleware, database, explorer, telnet, DNS, etc.
  - Employ cloud-based analysis engine
  - Allow custom IPS rules
  - Database update once a week
- **Certificate and partnership**
  - Common Vulnerabilities and Exposures (CVE) compatibility certificated
  - Microsoft Active Protections Program (MAPP) partnership

Risk Assessment and Security Service

- **Risk assessment**
  - Scan and identify security loopholes such as open port, system vulnerabilities, weak passwords, etc.
- **Web scanner**
  - On-demand scanning of targeted website/URL to discover the system vulnerabilities.
- **Real-time vulnerability scanner**
  - Discover vulnerabilities in real-time and protection against 0-days attacks
- **SANGFOR threat intelligence service**
  - Threat intelligence to deliver the latest vulnerabilities, malware and security incidents information with advisory alerts for policy creation

Web Application Firewall

- **Web-based attack prevention**
  - Support SNORT based and semantic detection engine to
  - Defend against the 10 top major web-based attacks identified by the Open Web Application Security Project (OWASP)
  - Web-based attack rules database
  - Support custom WAF rules
- **Parameters protection**
  - Proactive protection of automatic parameter learning
- **Application hiding**
  - Hide the sensitive application information to prevent hackers from mounting targeted attacks with the feedback information from the applications
- **Password protection**
  - Weak password detection and brute-force attack prevention
- **Privilege control**
  - File upload restriction of file type blacklist
  - Specify access privilege of sensitive URL such as the admin page for risk prevention
- **Buffer overflow detection**
  - Defend against buffer overflow attacks
- **Detection of HTTP anomalies**
  - Analyze anomalies of the fields of the HTTP protocol via single parsing
- **Secondary authentication for server access**
  - Server access verification by IP address restriction and mail authentication

Data Leakage Prevention

- **Data leakage detection and prevention**
  - Control and detection over multiple types of sensitive information (customizable)including user information, email account information, MD5 encrypted passwords, bank card numbers, identity card numbers, social insurance accounts, credit card numbers, and mobile phone numbers
- **File downloading control**
  - Restrict suspicious file downloading

User Access Management

- **User identity:**
  - Mapping by IP, MAC, IP/MAC binding, hostname and USB-Key. User account import from CSV file and LDAP Server.
  - SSO integration with AD domain, proxy, POP3 and WEB
- **Internet content classification**
  - Cloud-based URL/APP classification engine
- **Access control**
  - Policy configuration oriented toward users and applications for web filter, application control and bandwidth management

Visibility Reporting

- **Built-in report center**
  - Full visibility to network, endpoint and business servers with multi-dimensional analysis of risks, vulnerabilities, attacks, threats and behaviours
  - Threats analysis for specific attack by Description, Target, Solution
  - Support visualization into cyber kill chain
  - Business Systems based reporting
- **Report subscription**
  - Support PDF format and automatically send to pre-defined mailbox on daily/weekly/monthly basis

Deployment

- **Configuration Wizard**
  - Guideline for deployment and policy configuration
- **Deployment**
  - Gateway (Route mode) | Bridge mode | Bypass mode | Multiple Bridge mode (2- 4 bridges) | Virtual Wire
- **High Availability**
  - Active-Active | Active-Passive
- **Bypass**
  - Hardware bypass in the event of hardware failure
- **Central Management**
  - Support central management of multiple NGAFs
  - Support quick deployment from Central Management Console

نمایه شرکت

فن آوری های Sangfor پیشرو در زمینه فروش جهانی راه حل های زیرساخت فناوری اطلاعات ، متخصص در رایانش ابری و امنیت شبکه با طیف گسترده ای از محصولات و خدمات از جمله: زیرساخت Hyper-Converged، زیرساخت دسک تاپ مجازی ، فایروال نسل بعدی ، مدیریت دسترسی به اینترنت ، حفاظت از نقطه پایانی ، محافظت در برابر باج افزار است. محافظت ، شناسایی و پاسخ مدیریت شده ، بهینه سازی WAN ، SD-WANو بسیاری دیگر

Sangforنیازهای تجاری و تجربه کاربری مشتریان را جدی می گیرد و آنها را در قلب استراتژی شرکت ما قرار می دهد. نوآوری و تعهد مداوم در ایجاد ارزش برای مشتریان به آنها کمک می کند تا رشد پایدار داشته باشند. Sangforدر سال 2000 تأسیس شد ، در حال حاضر 5000 کارمند با بیش از 60 دفتر شعبه در سراسر جهان در مکانهای مهیج مانند هنگ کنگ ، مالزی ، تایلند ، اندونزی ، سنگاپور ، فیلیپین ، ویتنام ، میانمار ، پاکستان ، امارات متحده عربی ، ایتالیا و ایالات متحده دارد.

نوآوری مداوم و خدمات عالی

Sangforحداقل 20٪ از درآمد سالانه خود را در تحقیق و توسعه سرمایه گذاری می کند ، محصولات فعلی را بهبود می بخشد و راه حل های جدیدی را در چهار مرکز تحقیق و توسعه خود در ایالات متحده آمریکا و چین توسعه می دهد. تاکنون ، Sangforبرای بیش از 1000 حق ثبت اختراع با برنامه های ثبت اختراع بیشتر که برای سال 2020 برنامه ریزی شده است ، درخواست کرده است. این تعهد به نوآوری ، Sangforرا قادر می سازد نسخه های جدید و به روز شده محصولات را هر سه ماه یک بار منتشر کند و محصولات جدید را سالانه یا هر دو سال به بازار عرضه کند.

Sangforهمچنین بر خدمات عالی تأکید دارد. با سه مرکز خدمات مشتری در مالزی و چین ، کل ظرفیت خدمات مشتری Sangfor بیش از 250 تکنسین و ارائه دهنده خدمات است.

با داشتن هزاران مهندس مجاز و پشتیبانی آنلاین 24ساعته و 7 روز هفته در 365 روز سال ، مشتریان Sangfor از پشتیبانی سریع و شخصی خدمات در محل لذت می برند.

در حال حاضر ، Sangforبیش از 100000 مشتری در سراسر جهان دارد ، بسیاری از آنها 500 شرکت Fortune ، مؤسسات دولتی ، دانشگاه ها و مدارس هستند.

جوایز و دستاوردها

- "Technology Fast 500 Asia Pacific Region" Award for 8 consecutive years from 2005 to 2012 by Deloitte
- Sangfor SSL VPN No. 1 in Network Security market in China, Hong Kong & Taiwan according to F&S
- No. 1 for Secure Content Management Hardware and VPN Hardware segment in China according to IDC
- Sangfor NGAF WAF recommended by NSS labs (2014)
- "Most Promising Network Security Solution" in June 2016 by Singapore NetworkWorld Asia
- "Readers Choice Awards for Enterprise Security" in October 2016 by Computerworld Malaysia
- Member of various technology alliances including VirusTotal
- "Next Gen" Award for Sangfor Endpoint Secure by Cyber Defense Magazine (2019)
- SAP Certified for Cloud and Infrastructure Operations and SAP HANA Operations (2019)
- ICSA Labs certification for Sangfor Next Generation Firewall (2020)

تهران، خیابان شهید بهشتی ، خیابان پاکستان ، کوچه چهارم ، پلاک ۱۱ ، طبقه چهارم ، واحد ۷
تلفن: ۸۸۸۰۴۹۶۱ | دورنگار: ۸۹۷۸۳۷۳۷ | کدپستی : ۱۵۳۱۶۴۵۹۱۸
info@arka.ir
www.arka.ir
رایان سامانه آرکا