فایروال هوشمند حرفه‌ای

Hillstone®
NETWORKS

شرکت پرداد رایان پارس (نماینده فروش هیلستون در ایران)
تهران. میدان هفت تیر ، خیابان موسوی ، پلاک ۵۰
تلفن:۸۸۳۱۸۱۹۰ -۰۲۱ ۸۸۵۹۲۴۳۲-۰۲۱ | فکس: ۸۸۳۰۱۴۹۵ -۰۲۱
info@pardad.co | www.pardad.co

فایروال هیلستون

T1860 / T2860 / T3860
T5060 / T5860

آشنایی با هیلستون

شرکت هیلستون از شرکتهای پیشرو در ارائه فایروال در دنیا میباشد. فایروالهای هیلستون با کسب رتبه برتر NSS Labs و حضور چندساله در گارتنر امنیت سازمان شما را تامین مینمایند.

این شرکت در سال ۲۰۰۶ توسط کارمندان قدیمی و با تجربهCiscoوNetScreen و Juniper بنیان گذاشته شد. هیلستون در سال ۲۰۱۶ توانست نشان " Recommended NSS" را از آزمایشگاه NSS با درصد شناسایی ۹۹٪ بالاتراز رقبایی همچون جونیپر و پائولوآلتوکسب نماید.

محصولات این شرکت در لایه ورودی شبکه شامل فایروالهای نسل بعدی(Next Generation Firewalls) و فایروالهای نسل بعدی هوشمند میباشد. (Intelligent Next Generation Firewalls)

این محصولات با استفاده از یادگیری ماشینی و هوش مصنوعی رفتار داخل شبکه شما را به دقت بررسی نموده تا با تشخیص رفتارهای غیر عادی به متخصصان اجازه تایید یا بلوکه کردن آنها را بدهند.

محصولات شرکت هیلستون قابل استفاده در شرکتهای کوچک تا دیتاسنترهای بزرگ با حجم انتقال دیتای بسیار بالا میباشد. IPS فایروالهای هیلستون دارای جامعترین موتور بازرسی با کارایی بسیار بالا میباشند.

Hillstone NETWORKS

اضافه کردن خرد به امنیت

تهاجم‌های سایبری، با استفاده از حملات هدفمند، مداوم، مخفیانه و چند مرحله‌ای که به راحتی تمهیدات امنیتی سنتی را دور می‌زنند، پیشرفته‌تر و پیچیده‌تر شده‌اند. محصولات امنیتی هیلستون، از تکنولوژی رفتارشناسی برای مقابله با تهدیدات پیشرفته و ایجاد امنیت مستمر برای شبکه‌های امروزی استفاده می‌نمایند. این محصولات از خوشه‌بندی آماری برای تشخیص بدافزارهای ناشناخته و تجزیه تحلیل رفتاری برای تشخیص رفتارهای غیرمعمول در شبکه استفاده می‌کنند. سپس با استفاده از موتور آنالیز رخدادهای هیلستون، ارتباط بین این رویدادها را تعیین کرده و اطلاعات لازم جهت کشف و خنثی کردن تهدیدات را در اختیار شما قرار می‌دهند.

با قدرت تشخیص عمیق و قابلیت تجزیه و تحلیل تهدیدات، راه‌حل‌های هیلستون به مشتریان یک دید جامع نسبت به وضعیت ریسک شبکه و قابلیت تشخیص و جلوگیری از تهدیدات پیشرفته مانند Locky Ransomware را ارائه می‌دهد. امنیت چند لایه‌ای هیلستون از چندین موتور سطح بالا برای محافظت در مقابل ransomwareها استفاده می‌نماید: آنتی‌ویروس، موتور پیشگیری از نفوذ (IPS) تشخیص تهدید پیشرفته (ATD) تشخیص رفتار غیرعادی (ABD) اعتبار سنجی (RPD) و غیره.

با امنیت چند لایه‌ای خود، محصولات هیلستون می‌توانند پیچیده‌ترین تهدیدات را در در مرحله‌ای که باشند تشخیص داده و از بین ببرند.

تجزیه و تحلیل رفتار

هیلستون با استفاده از هوش مصنوعی، تحلیل داده های بزرگ و مدل‌سازی ریاضی/آماری، رفتار شبکه شما را ارزیابی کرده و علاوه بر تشخیص رفتار عادی شبکه شما،هرگونه رفتار خارج از عرف شبکه را به شما اخطار می‌دهد. علاوه بر این امکان تعریف عملیات از پیش تعریف شده جهت مقابله با حملات احتمالی میسر می‌باشد.

آنالیز حملات

هیلستون دارای ابزارهای زیادی برای کمک به مدیر شبکه جهت پیدا کردن ریشه حملات می‌باشد. گزارشات و لاگ‌های فراوان که توسط هیلستون به دسته‌های مختلف از آماده‌سازی حمله تا وقوع آن دسته‌بندی شده اند. دسته‌بندی سیستم‌های داخل شبکه بر اساس میزان آسیب‌پذیری در مقابل حملات، پکت‌های شبکه ذخیره شده و غیره همگی به آنالیز حملات انجام شده به سازمان شما کمک خواهند کرد.

کنترل نرم‌افزارها

هیلستون بدون وابستگی به پورت و پروتوکل، امکان مدیریت و کنترل نرم‌افزارهای مختلف را دارا می‌باشد. هیلستون می‌تواند خطرات ناشی از استفاده از نرم افزارهای دارای ریسک بالا را تشخیص داده و همچنین بر اساس سیاست‌های تعیین شده، نرم افزارها، کاربران و گروه‌های کاربری را کنترل نماید. علاوه بر این امکان کنترل پهنای باند مصرفی بر اساس نرم‌افزار نیز امکان‌پذیر می‌باشد.

رتبه‌بندی ریسک شبکه

تکنولوژی ثبت‌شده ایندکس گذاری ریسک شبکه‌ي هیلستون با پردازش دائمی پکت‌ها، لاگ‌ها و بررسی وضعیت سلامت شبکه، بصورت زنده رتبه شبکه‌ی شما را از لحاظ ریسک خطرات آن نمایش داده و با استفاده از داشبورد آن، امکان بررسی و رفع مشکلات امنیتی شبکه را برای شما امکان‌پذیر می‌نماید.

تشخیص بدافزارهای ناشناخته

هیلستون علاوه بر تشخیص بدافزارهای رایج از طریق مقایسه آن‌ها با بانک اطلاعاتی موجود خود، با استفاده از الگوریتم‌های پیچیده ریاضی، درصد شباهت دیتای رد شده از داخل خود را به یکی از بدافزارهای موجود تعیین کرده و بر اساس آن به شما امکان تصمیم‌گیری در مورد آن را می‌دهد. با استفاده از این سرویس امکان یافتن نسخه‌های مختلف ناشناخته از یک بدافزار امکان‌پذیر می باشد.

ابزارهای کاربری عالی

رابط کاربری هیلستون به شما امکان مشاهده و کنترل نرم‌افزارهای شبکه، ترافیک شبکه، کاربران و گروه‌ها، مصرف پهنای باند، رفتارهای مشکوک، رفتارهای غیرعادی، فاکتورهای ریسک‌پذیر شبکه، تهدیدهای درحال شکل‌گیری و بسیاری از عوامل دیگر را می‌دهد. ابزارهای زیادی نیز برای مانیتور کردن، گزارش‌گیری، خواندن لاگ‌ها، پیش‌بینی خطرات و غیره دارد.

فایروال‌های رده E

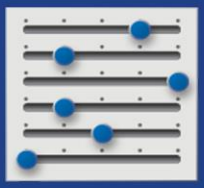
فایروال‌های سری E هیلستون به شما امکان بررسی و کنترل وب‌اپلیکیشن‌های مختلف را صرف نظر از پورت، پروتوکل و یا نوع فعالیت می‌دهد. این فایروال‌ها می‌توانندتهدیدات مربوط به نرم افزارهای دارای ریسک بالا را تشخیص داده و جلوگیری نمایند و بر اساس سیاست‌های تعیین شده، نرم‌افزارها، کاربران و گروه‌های کاربران را کنترل نمایند

سیاست‌ها را می‌توان به نوعی تعریف کرد که پهنای باند مورد نیاز برنامه‌های حیاتی مهم را تضمین نموده و در عین حال نرم‌افزارهای مخرب و غیرکاربردی را محدود و یا مسدود نمود. فایروال‌های سری E هیلستون، ترکیبی از امنیت جامع شبکه به همراه ویژگی‌های یک فایروال پیشرفته را به شما عرضه می‌کنند. این فایروال‌ها دارای قیمت عالی، راندمان بالا، و سایز کوچکتر در مقابل محصولات رقیب می‌باشند.

تشخیص و کنترل جامع تهدیدات

فایروال‌های سری E هیلستون، امکان محافظت بلادرنگ در مقابل برنامه‌ها و تهدیدات شبکه شامل باتنت‌ها،worm‌ها،ویروس‌ها، ابزارهای جاسوسی تروجان‌ها، ARP Spoofing، DoS/DDoS، SQL Injection و Buffer Overflows را فراهم می‌نماید. این فایروال‌ها شامل موتور چند منظوره تشخیص بدافزار می‌باشند که مشخصات پکت‌های دریافتی را با مدول‌های امنیتی دیگر مانند آنتی‌ویروس، IPS به اشتراک گذاشته که باعث URL Filtering و کاهش تاخیر در سرویس‌دهی می‌شود.

کنترل قسمت به قسمت نرم‌افزارها



فایروال‌های سری E هیلستون، امکان کنترل وب اپلیکیشن‌ها را صرفنظر از پورت، پروتوکل و نحوه فعالیت فراهم می‌آورد. این فایروال‌ها می توانندتهدیدات مربوط به نرم‌افزارهای دارای ریسک بالا را تشخیص داده و جلوگیری نمایند و بر اساس سیاست‌های تعیین شده، نرم‌افزارها، کاربران و گروه‌های کاربران را کنترل نمایند.

فایروال‌های رده T

فایروال‌های نسل بعدی هوشمند سری T هیلستون از سه تکنولوژی کلیدی برای تشخیص حملات پیشرفته و دفاع از شبکه‌های امروزی در مقابل آن‌ها بصورت مستمر استفاده می‌کند:

در ابتدا با استفاده از موتور پتنت شده تشخیص پیشرفته تهدیدات هیلستون (ATD) و با خوشه‌گذاری آماری، تهدیدات شناخته نشده جدید را کشف می‌نماید

دوم با استفاده از موتور تشخیص رفتار غیرعادی هیلستون (ABD) از تجزیه و تحلیل رفتاری برای پیدا کردن رفتارهای غیرعادی در شبکه استفاده می‌نماید

سوم با استفاده از موتور تجزیه و تحلیل تهدیدات، کلیه رویدادهای ثبت شده توسط سایر موتورها از جمله ATD، ABD، Sandbox و غیره بررسی شده و بعنوان یک گزارش کامل از تهدید به همراه راه‌حل آن ارائه می‌گردد.

تدابیر پیشگیرانه

هیلستون علاوه بر توانایی تغییر قانون برای جلوگیری از حمله، چندین ویژگی خوکار بازدارنده داخلی دارد. این ویژگی ها شامل قالب های از پیش تعریف شده ای است که به صورت خودکار در صورت شناسایی رفتار مشکوک، باعث کاهش سرعت و یا بلوکه کردن حمله می شوند. مدیر می تواند این قالب ها را جهت محدود کردن پهنای باند یا کاهش تعداد سشن های در اختیار مهاجم، تغییر دهد. او همچنین می تواند محدودیت های خود را بر منابع شبکه بر اساس نوع حمله و شدت آن تنظیم کند. در مواردی که حمله بحرانی است و سطح اطمینان بالا می‌باشد، عکس‌العمل می تواند شامل انسداد کامل تمام منابع شبکه باشد. و اگر قالبی وجود ندارد یا غیر فعال است، مدیر می تواند به سرعت تغییرات موقتی را برای آن رویداد تنظیم کند .

تشخیص بدافزارهای ناشناخته

هیلستون دارای یک موتور اختصاصی می‌باشد که نزدیک به یک میلیون نمونه شناخته شده را آنالیز کرده است. هر نمونه بر اساس ابعاد مختلف که شاخص‌های مختلف آن را توصیف می‌نماید، طبقه بندی و مشخص شده‌اند. در محیط واقعی، زمانیکه بدافزار جدید یافت می‌شود، به همین‌صورت آنالیز و طبقه‌بندی می‌شود. سپس با بانک بدافزارهای شناخته شده که قبلا آنالیز و طبقه‌بندی شده‌اند مقایسه می‌شود. هرچه این بدافزار به نمونه‌های قبلی نزدیکتر باشد، امکان اینکه گونه جدیدی از آن بدافزار باشد بیشتر است. به این روش خوشه‌بندی آماری گفته می‌شود که راه دقیقی برای شناختن تهدیدات جدید می‌باشد .

تشخیص رفتارهای غیرعادی

موتور بررسی رفتار غیرعادی هیلستون بطور دائم شبکه را جهت یادگیری رفتار نرمال شبکه بر اساس روز، ساعت و ماه زیر نظر داشته و در صورت مشاهده رفتار خارج از عرف، هشدار خواهد داد. این موتور از یک آرایه با بیش از 50 بُعد جهت بررسی رفتار شبکه استفاده می‌کند که به آن مدل‌سازی رفتاری می‌گویند. علاوه بر این، این موتور توسط ابزارهای هک مختلف آموزش داده شده است تا اطمینان حاصل شود که رفتارهای مخرب را شناسایی خواهد کرد. این تکنیک از تشخیص‌های اشتباه جلوگیری کرده و باعث می‌شود که کاربر راه‌حل‌های متنوعی برای جلوگیری از حملات داشته باشد .

آنالیز و تحلیل قوی

هیلستون روش جدیدی را برای تجسم و تحلیل حملات ارائه می دهد.هر اقدامی که توسط یک کد مخرب بالقوه انجام می شود به طور خودکار به مراحل درون "زنجیره کشتار" ربط داده می‌شود. این اقدامات با اطلاعات قانونی تکمیل می‌شود که تحلیلگر امنیتی را قادر می سازد تا مبدأ حمله، شدت حمله و روش شناسایی مورد استفاده را تعیین کند. هیلستون همچنین فایل هایی از پکت های ضبط شده را فراهم و لاگ های syslog می کند، که در صورت ترکیب با ترافیکی، مدیر را با گنجینه‌ای از اطلاعات اضافی همراه می کند . علاوه بر این، داده های کاربر مانند وب سایت های بازدید شده ، برنامه های کاربردی مورد استفاده، و سطح خطر برنامه ها، باعث تمرکز بر روی خطرات آن ها خواهد شد. مهمتر از همه، هیلستون قانونی را که به مهاجم اجازه عبور از فایروال را داده است را شناسایی می‌نماید.

تایید شده توسط:

vmware | amazon web services Partner Network | Microsoft | Alibaba Cloud

openstack | MIRANTIS Pure Play OpenStack | CITRIX | big switch networks

algosec | FIREMON PROACTIVE SECURITY INTELLIGENCE | CYPHORT Advanced Malware Defense | TREND MICRO

فایروال‌های رده x

فایروال دیتاسنتر مدل X7180 هیلستون دارای عملکرد فوق العاده، قابلیت اطمینان بسیار بالا و مقیاس پذیری برای ارائه دهندگان خدمات با سرعت بالا، شرکت های بزرگ و شبکه های حامل است. این محصول امنیت انعطاف پذیری را برای محیط های چندرسانه‌ای مبتنی بر کلاود و امنیت به عنوان یک سرویس، فراهم می کند

پلت فرم X7180 بر اساس معماری امنیتی ELASTIC هیلستون(ESA)می‌باشد که اجازه ایجاد فایروال‌های مجازی بسیار مقیاس پذیر، THROUGHPUT بسیار بالا، سشن‌های همزمان بسیار و سشن جدید در ثانیه بسیار زیاد ارائه می دهد. همچنین X7180 دارای DPI ، کنترل نرم‌افزارنسل بعدی QOS و می‌باشد. این محصول عملکرد استثنایی خود را در یک قالب کوچک با مصرف انرژی پایین ارائه می‌دهد

با افزایش سرویس‌های ارائه شده بر روی اینترنت و بالا رفتن تعداد کاربران آن ترافیک دیتاسنترها افزایش پیدا می‌کند. این موضوع اهمیت تجهیزات شبکه با سرعت بالا و تراکم پورت بیشتر را افزایش می‌دهد. افزایش تعداد کاربران موبایل نیاز دیتاسنترها را به سمت تجهیزات امنیتی که تعداد کاربران زیاد با پکت‌های کوچک را پشتیبانی می‌کنند سوق داده است. بنابراین یک فایروال دیتاسنتر باید THROUGHPUT بالا، سشن‌های همزمان بسیار زیاد و سشن در ثانیه بسیار بالا را پشتیبانی نماید. از همه مهمتر، این فایروال‌ها باید بتوانند پاسخگوی الگوی مصرف کاربران خود که در اکثر موارد غیرقابل پیش‌بینی هستند باشند. در نتیجه فایروال‌ها باید قابلیت ارتجاعی و ارائه امنیت بر اساس نیاز مشتری را داشته باشند

بهره‌وری در انرژی

فایروال X7180 دارای اسلات در جلو و عقب خود می‌باشد که باعث صرفه‌جویی در فضای رک و نیاز کمتر به خنک شدن می‌شود. فضای مورد نیاز برای این فایروال 5 یونیت می‌باشد و توان مصرفی آن که نسبت به فایروال‌های مشابه 50 تا 1500W 67 درصد کمتر است.

تدابیر پیشگیرانه

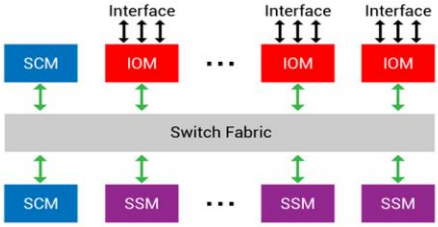
پلتفرم X7180 می تواند پهنای باند مصرفی را بر اساس برنامه‌ها، کاربران و زمان روز مدیریت کند. این سیستم، سیاست‌های شما را بطور دقیق برمبنای پهنای باند تضمین شده، اعمال محدودیت بر پهنای باند، که می‌تواند بصورت FlexQOS اولویت‌بندی ترافیک و پویا پهنای باند را بر اساس بار سیستم تنظیم نماید، اعمال می‌کند.

اطمینان در سطح کریر

فایروال X7180 یک فایروال قابل اطمینان برای دیتاسنترها می‌باشد. این فایروال با پشتیبانی از HA در هر دو حالت active/passive و active/active به‌شما اطمینان فعالیت بصورت24x7 را می‌دهد. این فایروال همچنین دارای منبع تغذیه، فن ،SCM، SMM و IOM ،ریداندنت وHot pluggable می‌باشد. فایروال X7180 همچنین دارای مدول bypass فیبر single-mode و multi-mode برای تداوم فعالیت در هنگام قطع شدن برق می‌باشد.

IPv6 و NAT

گذر اجتناب ناپذیر به سمت IPv6 در حال انجام است ولی دیتا سنترها کماکان نیازمند به NAT در سطح کریر (LSN) Large Scale NAT و (CGN) برای مدیریت کمبود IPv4 در هنگام این انتقال می‌باشند. فایروال X7180 از تکنولوژی‌های مختلفی از جمله IPv6/IPv4 tunnels, DNS64/NAT64, NAT 444, full cone NAT, NAPT , Dual Stack, و غیره بهره می‌گیرد. لاگ‌گیری از سشن‌ها و جداول تبدیل آی‌پی امکان ممیزی فعالیت‌های انجام شده را می‌دهد.



فایروال مرکز داده X7180 بر اساس معماری امنیتی الاستیسیته هیلستون ساخته شده است. این فایروال می تواند تا 1000 فایروال مجازی را پشتیبانی کند و می تواند برای ارائه سرویس بر اساس درخواست مشتری، همراه با توافق نامه شرایط ارائه سرویس (SLA) استفاده شود. ارائه دهندگان سرویس می‌توانند منابع فایروال از قبیل CPU، تعداد سشن‌ها، سیاست‌ها و پورت‌ها را بر اساس SLA تعیین شده برای هر فایروال مجازی بصورت پویا تعیین نمایند.

سخت‌افزار فایروال X7180 هیلستون متشکل از چندین لبه شبکه و امنیتی می‌باشد که اجازه مقیاس‌پذیری آن را برای آینده می‌دهد. معماری چند هسته‌ای توزیع شده آن امکان سرویس‌دهی با throughput 680Gbps و ۲۴۰ میلیون سشن همزمان و ۴/۸ میلیون سشن جدید در ثانیه را می‌دهد. بدنه این فایروال ۶۸ پورت 10GbE یا ۱۴۴ پورت 1GbE را پشتیبانی می‌نماید.

جوایز و نشان ها:

14,000+ مشتری که hillstone را جایگزی cisco , juniper , ... کرده اند:

موسسات دولتی
1800+ Government agencies

موسسات مالی
Top 5 China State Owned Banks, *Big 3* stock exchanges
Top 10 securities dealers, *Top 5* insurance groups

مراکز آوزشی
200+ colleges
600+ educational institutes

ISP
60% market share of China Broadband SPs
5-Yrs on China Telecom, China Mobile Short Lists

ICP
100+ ICP

سایر
6000+ Enterprise and SMB customers
30+ countries

فایروال هوشمند حرفه‌ای

Hillstone NETWORKS

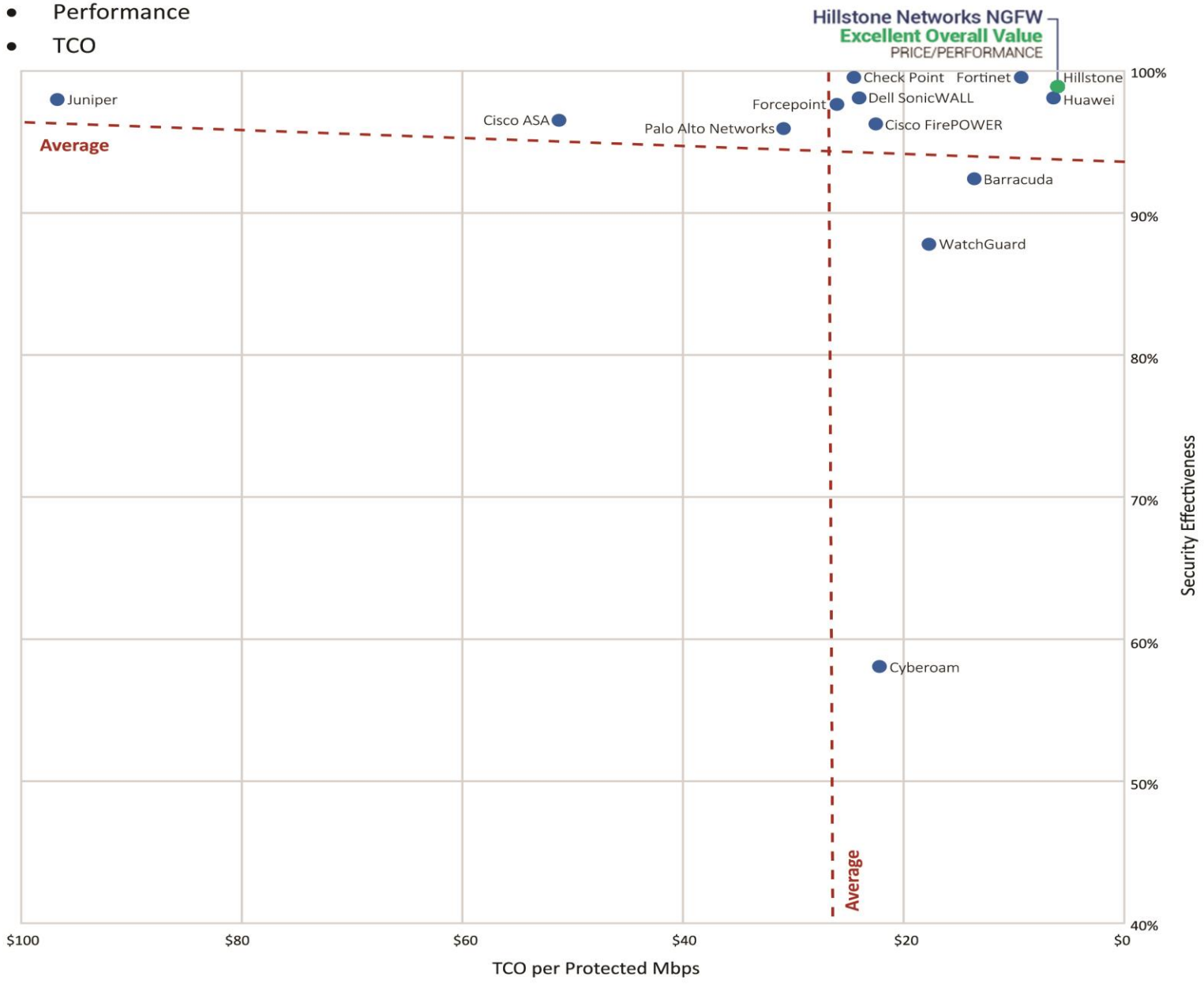
مقایسه Hilstone با سایر فایروالها
توسط آزمایشگاه NSS LAB

شرکت پرداد رایان پارس (نماینده فروش هیلستون در ایران)
تهران. میدان هفت تیر ، خیابان موسوی ، پلاک ۵۰
تلفن:۰۲۱- ۸۸۳۱۸۱۹۰ ۰۲۱-۸۸۵۹۲۴۳۲ | فکس: ۰۲۱- ۸۸۳۰۱۴۹۵
info@pardad.co | www.pardad.co

رتبه یک در NSS LAB
(قیمت در برابر امنیت)

Overview

- Security
- Performance
- TCO



NSS Labs 2016 Security Value Map (SVM) for Next Generation Firewall (NGFW)

NSS LABS RECOMMENDED

99.60%
Block Rate in Static test

98.32%
Block Rate in Live Test