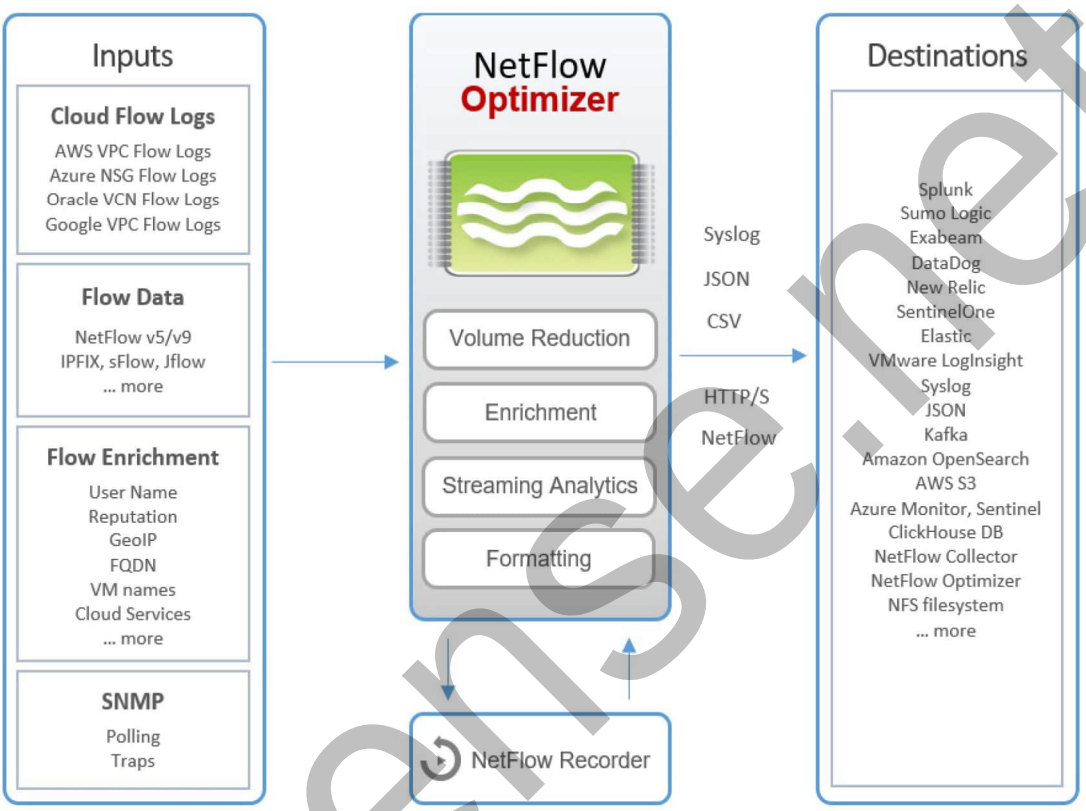
بهینه‌ساز ترافیک شبکه NETFLOW

با NETFLOW OPTIMIZER میتوانید جریان‌های داده را بهینه‌سازی و غنی کرده و عملکرد شبکه خود را به‌آسانی تحلیل کنید.

NETFLOW OPTIMIZER به شما این امکان را می‌دهد تا حجم گسترده‌ای از داده‌های NETFLOW، IPFIX، SFLOW، لاگ‌های جریان CLOUD VPC و موارد مشابه را پردازش کنید. این پلتفرم داده‌ها را بهینه‌سازی و در زمان واقعی غنی‌سازی می‌کند تا اطمینان یابید که اطلاعات موردنیاز را در مکان‌های تعیین‌شده و قالب‌های مناسب دریافت می‌کنید.



مزایای کاهش حجم داده‌های در جریان

کاهش حجم داده‌های در جریان مانند NETFLOW در سامانه‌های نظارت بر شبکه از اهمیت بالایی برخوردار است. این اقدام به دلایلی همچون کاهش بار سیستم، صرفه‌جویی در فضای ذخیره‌سازی، و بهبود کارایی تحلیل‌ها صورت می‌گیرد. در ادامه، هر یک از روش‌های کاهش حجم داده به‌تفصیل بررسی خواهد شد.

حذف داده‌های تکراری (DEDUPLICATION):

در صورتی که یک جریان شبکه‌ای توسط چندین دستگاه گزارش شود، تنها یک نسخه از آن در سیستم ذخیره می‌شود. این روش از تکرار اطلاعات جلوگیری کرده و به طور قابل توجهی حجم داده‌ها را کاهش می‌دهد.

تجمیع داده‌ها (CONSOLIDATION):

جریان‌های مشابهی که در یک بازه زمانی مشخص بین دو دستگاه تبادل می‌شوند، به یک جریان واحد تبدیل می‌گردند. این فرایند از طریق جمع‌بندی اطلاعات مرتبط با این جریان‌ها انجام می‌شود و علاوه بر کاهش حجم داده‌ها، به تحلیل‌های جامع‌تر نظیر شناسایی الگوهای ترافیکی کمک می‌کند. استفاده از این روش می‌تواند حجم داده‌ها را تا 80 درصد کاهش دهد.

فیلتر کردن جریان‌های برتر (TOP TRAFFIC FILTERING):

با تمرکز بر جریان‌های کلیدی و پیکربندی سیستم برای ذخیره‌سازی تعداد مشخصی از جریان‌های مهم (به عنوان مثال N جریان برتر)، می‌توان حجم داده‌ها را به میزان قابل توجهی کاهش داد. این روش با حذف جریان‌های کم‌اهمیت، ضمن کاهش حجم داده‌ها، دقت تحلیل‌ها را تا 99 درصد حفظ می‌کند. در بسیاری از موارد، این روش قادر است حجم داده‌ها را تا 95 درصد یا بیشتر کاهش دهد. به عنوان نمونه، اگر N برابر با 1000 در نظر گرفته شود، تنها 1000 جریان با بیشترین حجم در سیستم ذخیره می‌شوند.

افزایش اطلاعات جریان داده

افزودن اطلاعات تکمیلی به رکوردهای NETFLOW

- نام‌های DNS و نام ماشین‌های مجازی
- هویت کاربران
- نام نمونه‌های ابری، خدمات، و مناطق جغرافیایی
- داده‌های حاصل از نظرسنجی‌های SNMP
- موقعیت جغرافیایی بر اساس کشور یا شهر
- ایجاد لیست‌های تهدیدات و تشخیص زودهنگام تهدیدات

ترکیب رکوردهای جریان برای مکالمات کلاینت-سرور

ترکیب رکوردهای جریان مربوط به مکالمات خاص

گزارش وضعیت مکالمات شبکه شامل شروع، ادامه و پایان ارتباط‌ها : ارائه اطلاعات دقیق درباره زمان‌بندی شروع، ادامه، پایان و مدت‌زمان هر مکالمه شبکه‌ای

استفاده از یادگیری ماشین برای ارتقای امنیت و پایداری شبکه: شناسایی حملات DDOS با بهره‌گیری از تکنیک‌های یادگیری ماشین پیش‌بینی مشکلات احتمالی و خرابی‌های شبکه برای پیشگیری و بهبود عملکرد سیستم

مزایای کاهش حجم داده‌های در جریان

نظارت بر لاگ‌های جریان ابری

ویژگی‌های پیشرفته برای پردازش و غنی‌سازی لاگ‌های جریان در محیط‌های ابری

AWS :

- قابلیت خواندن لاگ‌های جریان VPC از منابع مختلف مانند CLOUDWATCH ، KINESIS، یا S3
- پشتیبانی از چندین حساب VPC ، AWS، و مناطق مختلف با استفاده از یک نمونه EC2 NFO
- غنی‌سازی رکوردهای جریان با افزودن اطلاعاتی مانند نام VPC ، نام نمونه EC2 ، نام DNS و منطقه AWS

AZURE :

- امکان خواندن لاگ‌های جریان NSG (NETWORK SECURITY GROUP)
- پشتیبانی از چندین حساب ذخیره‌سازی AZURE
- دسترسی به لاگ‌های جریان NSG از طریق اصل سرویس یا هویت مدیریت‌شده اختصاص‌یافته به سیستم
- غنی‌سازی رکوردهای جریان NSG با افزودن جزئیاتی مانند نام شبکه مجازی، نام ماشین مجازی، نام DNS و منطقه AZURE

GCP :

- قابلیت خواندن لاگ‌های جریان VPC در GOOGLE CLOUD PLATFORM
- پشتیبانی از چندین حساب سرویس GCP و پروژه
- غنی‌سازی رکوردهای جریان VPC با افزودن اطلاعاتی مانند نام شبکه VPC ، نام زیرشبکه، نام نمونه، نام DNS و منطقه GCP

این ویژگی‌ها امکان تحلیل دقیق‌تر و مدیریت بهتر جریان‌های داده در محیط‌های چندابری را فراهم می‌کند.

نظارت بر سلامت دستگاه‌های شبکه

شناسایی و تحلیل عملکرد شبکه با استفاده از روش‌های پیشرفته

شناسایی میزبان‌ها و دستگاه‌های شبکه با بیشترین ریست‌های TCP: تشخیص دستگاه‌ها یا میزبان‌هایی که بیشترین تعداد ریست‌های TCP را تجربه کرده‌اند، به منظور شناسایی مشکلات احتمالی ارتباطی.

تشخیص فشار بیش‌ازحد بر سیستم یا شبکه: شناسایی موقعیت‌هایی که نشان‌دهنده وجود فشار غیرعادی یا ترافیک بالا در یک سیستم یا شبکه است.

جمع‌آوری داده‌های دوره‌ای با پروتکل SNMP: استفاده از پروتکل SNMP برای جمع‌آوری اطلاعات منظم از دستگاه‌های شبکه به منظور پایش عملکرد و شناسایی مشکلات بالقوه.

این روش‌ها به بهبود کارایی و پایداری شبکه کمک کرده و امکان شناسایی زودهنگام مشکلات را فراهم می‌کنند.

توانایی دیدن و درک دقیق ترافیک شبکه با FLOW DATA

توانایی مشاهده و تحلیل ترافیک شبکه:

این ویژگی به شما امکان می‌دهد تا ترافیک شبکه را مشاهده و تحلیل کنید. با استفاده از داده‌های در جریان شبکه از منابع مختلف همچون:

لاگ‌های جریان VPC در AWS

دستگاه‌های شبکه PALO ALTO NETWORKS

دستگاه‌های امنیتی شبکه CISCO ASA

دستگاه‌های تولیدکننده سیسکو AVC (APPLICATION VISIBILITY AND CON-TROL)

هر صادرکننده‌ای که بر اساس پورت‌های مقصد شناخته می‌شود

این اطلاعات به شما کمک می‌کنند تا به طور دقیق‌تر و جامع‌تر وضعیت شبکه خود را نظارت کرده و مشکلات را شناسایی کنید.

امنیت

شناسایی تهدیدات امنیتی و ردیابی منابع تهدید شناخته‌شده:

شناسایی تهدیدات امنیتی موجود و پیگیری منابع تهدید شناخته‌شده فعلی به منظور مدیریت و پاسخگویی سریع.

غنی‌سازی داده‌های در جریان با اطلاعات موقعیت جغرافیایی و شهرت IP:

با افزودن اطلاعات مربوط به شهرت و موقعیت جغرافیایی IP، داده‌های در جریان شبکه غنی‌سازی می‌شود تا دید دقیق‌تری از تهدیدات احتمالی به دست آید.

بررسی دقیق میزبان‌ها:

تحلیل دقیق برای شناسایی میزبان‌هایی که تحت تأثیر تهدیدات امنیتی قرار گرفته‌اند.

این فرآیندها به شما کمک می‌کند تا تهدیدات امنیتی را سریع‌تر شناسایی کرده و به طور مؤثرتر آن‌ها را مدیریت کنید.

دید کامل شبکه برای مشتریان

VMWARE و SPLUNK، SUMO LOGIC، EXABEAM، ELASTIC

شناسایی و تحلیل تأثیرات شبکه بر عملکرد ماشین‌های مجازی (VM)

مشخص کردن دستگاه‌ها و رابط‌های فیزیکی:

شناسایی دستگاه‌ها و رابط‌های فیزیکی که بر عملکرد ماشین‌های مجازی (VM) تأثیر می‌گذارند و نمایش این اطلاعات در داشبورد SPLUNK.

بازسازی مسیرهای ارتباطی:

بازسازی و نمایش مسیرهای مکالمه بین ماشین‌های مجازی (VM-TO-VM) و ماشین‌های مجازی به میزبان (VM-TO-HOST) از طریق شبکه فیزیکی زیرساخت، برای تحلیل دقیق‌تر و شفاف‌تر جریان‌های شبکه.

این قابلیت‌ها امکان نظارت جامع‌تر و بهینه‌سازی عملکرد شبکه و ماشین‌های مجازی را فراهم می‌کنند.

عملکرد بی‌نظیر

قابلیت پردازش 1 میلیون جریان در ثانیه بدون افت

قابلیت پردازش تا 350 هزار جریان در ثانیه با ادغام

کار با هر نوع داده جریان

قادر به پردازش هر پروتکل استاندارد جریان

NETFLOW V5/V9، FLEXIBLE NETFLOW

IPFIX با فیلدهای متغیر و سازمانی

SFLOW (هم رکوردهای داده و هم رکوردهای شمارنده)

J-FLOW، CITRIX APPFLOW، NETSTREAM و غیره

کار با داده‌های SNMP

ارائه قابلیت‌های نظرسنجی SNMP با انعطاف‌پذیری بالا و امکان گسترش برای پوشش نیازهای مختلف شبکه

امکان دریافت و مدیریت تله‌های SNMP برای نظارت بر رخدادهای شبکه و پاسخگویی سریع به مشکلات.

ضبط کننده NETFLOW

ضبط کننده NetFlow ابزاری است که به شما امکان می‌دهد ترافیک شبکه را در یک بازه زمانی مشخص ضبط کرده و برای تحلیل‌های بعدی ذخیره کنید. این ابزار مانند یک دستگاه ضبط ویدیو عمل می‌کند که به جای تصویر، اطلاعات مربوط به جریان‌های شبکه (Flows) را ضبط می‌کند.

این رکوردها را به صورت syslog یا JSON به SIEM خود ارسال کنید تا دید کاملی از ترافیک شبکه گذشته کسب کنید.