Flowmon: Casi D’uso

La tua rete, gli applicativi e i database sono performanti e protetti come vuoi? Il tuo traffico di rete è davvero il tuo?

Il monitoraggio di rete ti fornisce una piena “visibilità” e una “sicura” analisi comportamentale.

Angelo Sbardellini

BDM Italy e Malta

Flowmon
Driving Network Visibility

Categories Overview

- Casi d'uso e le storie di successo sono organizzati in gruppi in base ai problemi da risolvere

- **Prestazioni e problemi operativi**
  - Problemi di configurazione
  - Errori di sistema
  - Bassa visibilità della rete/dell’applicazione

- **Sicurezza**
  - Malware
  - Botnets
  - Attacchi e distribuzione SPAM
  - Applicazione indesiderate, perdita dei dati e comportamento degli utenti

Prestazioni e problemi operativi

Problemi di configurazione

Flowmon
Driving Network Visibility

Configurazione del firewall errata

Il server principale ERP ha mostrato tempi di **risposta lunghi** per tutte le operazioni. Il produttore del sistema ERP ha cercato di ottimizzare il sistema per 14 giorni.

L'applicazione di Flowmon ha rilevato che un firewall configurato in modo errato caricava costantemente il server ERP con query non necessarie.

Il problema di prestazioni **è stato rimosso** tramite **una semplice regolazione della configurazione del firewall.**

(Vendita all'ingrosso)

Problemi di configurazione

Backup durante l'orario di lavoro

La rete dati ha mostrato **risposte molto lente** su tutti i sistemi ogni giorno **verso mezzogiorno.**

La causa di questo problema non è stata identificata per molto tempo e quindi è stato preso in considerazione **l'upgrade della dorsale a 10 Gpbs.**

Il monitoraggio del traffico tramite la soluzione Flowmon ha dimostrato che alcuni sistemi di produzione vengono sottoposti a **backup in orari errati** durante l'orario di lavoro anziché in quello notturno.

Il problema è stato risolto con una semplice regolazione del tempo di backup.

Problemi di configurazione

(Information technology)

Flowmon
Driving Network Visibility

Ritardi nella produzione

Ogni volta dopo le 7:00, si sono verificati dei ritardi nella produzione guidata da SAP. La causa del problema che ha avuto **conseguenze economiche reali** non era stata chiara.

L'analisi eseguita dalla soluzione Flowmon ha rilevato un carico estremo della rete dati verificatasi a causa dell'attività di controllo di gestione delle stazioni terminali e delle applicazioni.

Il sistema ha sempre contattato tutte le stazioni gestite e scaricato tutti i registri delle ultime 24 ore alle 7:00.

Una semplice modifica della configurazione e la diffusione di questa attività in un intervallo di tempo più ampio hanno eliminato il problema.

Problemi di configurazione

(Industria alimentare)

Registrazione troppo dettagliata

Un produttore nel settore automobilistico ha riscontrato **risposte inaspettatamente lunghe** nella rete di produzione.

Comuni controlli fatti con l'aiuto di strumenti come Simple Network Management Protocol (SNMP) e Firewall hanno confermato alcuni accumuli di traffico **ma non sono stati in grado di scoprire la causa**.

L'implementazione di Flowmon ha immediatamente indicato che **uno dei server** che fanno parte del sistema di produzione **invia giornalmente volumi di dati, in termini di gigabyte, alla sede centrale.**

Il server specifico invece di inviare dati complessivi aggregati, inviava i registri di produzione completi che **non era la configurazione desiderata.**

Problemi di configurazione

(Automotive)

Flowmon
Driving Network Visibility

Prestazioni e problemi operativi

Errori di sistema

Flowmon
Driving Network Visibility

Errore Software del firewall

Ritardi significativi nella comunicazione della rete internet si sono verificati a intervalli casuali.

A prima vista sembrava che uno degli utenti avesse scaricato enormi quantità di dati.

L'analisi tramite la soluzione Flowmon ha rivelato **un problema di firewall** che **termina la comunicazione** dell'utente alla pagina Web **in modo errato** e avvia l'invio di flussi di dati assurdamente grandi all'utente.

(Settore Sanitario)

Memoria di dati visivi

In alcuni casi, la risonanza magnetica **non è stata in grado di salvare la documentazione visiva del** paziente nell'archivio dati esterno gestito da uno degli appaltatori. I fornitori di entrambi i sistemi hanno dato la responsabilità alla rete di dati dell'ospedale. Come prova di questa affermazione errata, la registrazione della comunicazione tra i due sistemi **ha dimostrato che il problema non si trova nella rete dati**. I fornitori di entrambi i sistemi sono successivamente riusciti a eliminare il problema.

(Ospedale)

Perdita di connettività con le filiali

Diversi problemi di connettività tra la sede centrale e le sue filiali sono stati segnalati di giorno in giorno.

Il fornitore di connettività dati **ha aumentato la capacità della linea**, ma non ha funzionato.

L'implementazione di Flowmon ha scoperto che il terminale **di monitoraggio e gestione remota** ha iniziato a generare grossi trasferimenti di dati tra le stazioni e il server centrale subito dopo l'ultimo aggiornamento.

Questa situazione è stata successivamente risolta insieme al fornitore del sistema.

(Telecommunications)

Prestazioni e problemi operativi

Bassa visibilità della rete/dell’applicazione

Flowmon
Driving Network Visibility

Caso d'uso: no APM in uso

- Gli utenti di internet banking chiamano helpdesk con reclami riguardanti la velocità di applicazione
- L'helpdesk vede solo le luci verdi sugli schermi di monitoraggio dell'infrastruttura
- Risposta agli utenti: il problema non è dalla nostra parte

Risultato: clienti annoiati che condividono la propria esperienza sui social network

Caso d'uso: l'APM in azione

- Gli utenti di internet banking chiamano helpdesk con reclami riguardanti la velocità di applicazione
- L'helpdesk ha già ricevuto notifica da APM che la sezione "Generazione estratto conto" sta riscontrando un tempo di risposta di 20 secondi
- Risposta agli utenti: siamo a conoscenza della situazione, i nostri team stanno semplicemente lavorando sulla risoluzione e il servizio tornerà alla normalità in mezz'ora

Risultato: clienti soddisfatti

Flowmon APM benefici

Marketing

- Qual è il livello di performance per i clienti top?
- Quante persone sono state colpite dai nostri recenti tempi di inattività?
- Chi ha visto un errore 404 e come possiamo utilizzarlo per l'up-sell?
- Quali sono i principali motivi che portano ad abbandonare l'uso dell'applicazione?
- Come ottimizzare la base applicativa sui soliti schemi utente?

IT Management

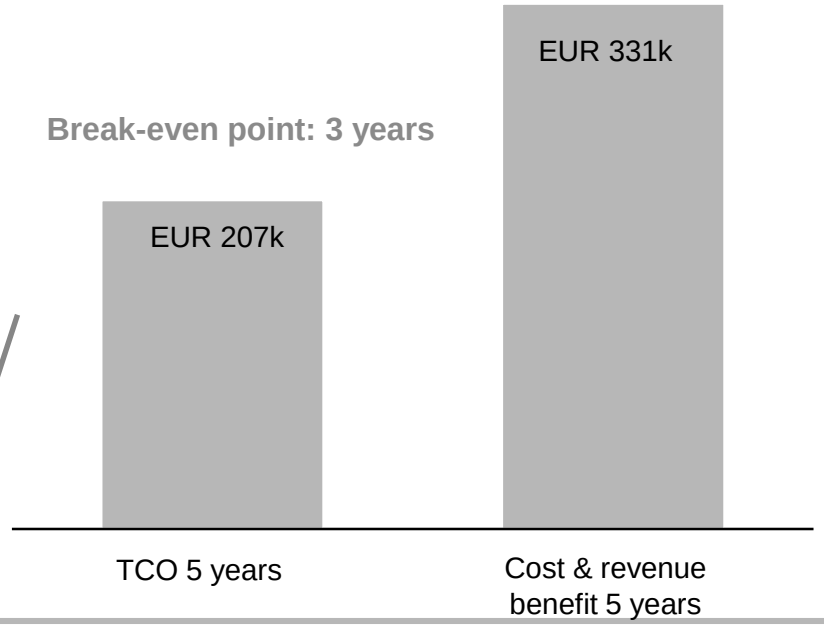
- I nostri fornitori soddisfano i nostri SLA?
- Quali elementi HW dovrebbero essere aggiornati?

IT Operations

- i nostri SLAs sulle performance soddisfano i nostri clienti enterprise?
- Quale fase della transazione commerciale sta causando i problemi?
- Qual è la differenza nelle prestazioni tra il front e back-end in base al tipo di richiesta?

IT Development

- Qual è stata la serie di transazioni che portano un utente a un errore?
- Qual è la performance delle nuove versioni prima che entri in produzione?



Principale punti di Ipotesi:
Il 10% degli utenti incontra un tempo di risposta> 5 sec
0,5% chiama helpdesk
Pagina di abbandono dello 0,5%
Miglioramento del 50% a causa di azioni correttive basate sulle informazioni APM Flowmon
costo medio del servizio di assistenza telefonica EUR 7,5, -
margine medio perso alla vendita incrementale 7,5 EUR, -

Flowmon
Driving Network Visibility

Sicurezza

Malware

Flowmon
Driving Network Visibility

Nuovo tipo di infezione da malware

Un rappresentante di vendita **è tornato da un viaggio di lavoro** dall'Asia. Una volta che il suo notebook è stato collegato alla rete dati della sua organizzazione, la soluzione Flowmon ha immediatamente **rilevato un comportamento non standard sul suo laptop** e quindi l'amministratore di sistema è stato automaticamente informato.

L'analisi successiva del laptop ha rivelato **un malware sotto forma di una libreria DLL**, che è stata introdotta durante l'avvio del sistema**.**

La firma di questo malware ha iniziato a comparire nel sistema antivirus dopo circa una settimana. Quindi è stato ancora considerato come un malware sconosciuto al momento del rilevamento.

malware

(Automotive)

Intercettazione del traffico dati

Grazie alla soluzione Flowmon, abbiamo rilevato un dispositivo **gravemente infetto** all'interno della nostra rete.

È stato un comunissimo laptop **in grado di reindirizzare la comunicazione** di un gran numero di dispositivi su Internet a se stesso.

Stava agendo come un GATE **e il malware poteva quindi sfruttare questa comunicazione**, ottenere le password, eventualmente anche reindirizzare l'utente a siti Web fraudolenti.

Abbiamo risolto l'incidente entro un'ora grazie al rilevamento automatico tramite Flowmon ADS.

malware

(Services/Retail)

Errore antivirus

Anche se utilizziamo un programma antivirus, l'analisi del traffico Flowmon della rete dati ha rilevato **due stazioni infette**.

È stato un malware comune ma gli antivirus **non erano stati aggiornati a causa del fallimento della funzione di aggiornamento automatico** e quindi non avevano avuto modo di rilevare l'infezione.

malware

(Governo)

Malware avanzato

La soluzione Flowmon ci ha comunicato che una stazione nella Repubblica Ceca ha iniziato **a utilizzare un server DNS in Russia**.

Questa segnalazione è stato visto come molto sospetta.

Si è rivelata **un'infezione da malware di tipo DNS Changer ,** a causa della quale un utente malintenzionato può reindirizzare gli utenti a siti Web fraudolenti.

Questo è un attacco molto sofisticato che può essere notato solo sulla stazione attraverso una modifica del server DNS.

malware

(Information technology)

Flowmon
Driving Network Visibility

Sicurezza

Botnets

Flowmon
Driving Network Visibility

Rivelamento di nuove botnet

Il monitoraggio della rete tramite la soluzione Flowmon ha mostrato una **tendenza crescente nel traffico telnet.**

Inoltre, questo traffico è stato collegato ai dispositivi, **dove non si è mai verificato prima.**

È stata rilevata una **nuova botnet**, successivamente contrassegnata come "**Chuck Norris**".

La soluzione Flowmon ha quindi contribuito in modo significativo all'analisi del suo comportamento e alla rivelazione del meccanismo di comando e controllo.

Database di qualità sulla reputazione IP

Un responsabile della sicurezza di un istituto finanziario ha dichiarato che la componente ADS di Flowmon ha rilevato **una comunicazione tra Botnet command e centro di controllo**, che **un altro strumento di sicurezza in uso non ha notato**.

Abbiamo confermato l'infezione attraverso l'analisi successiva.

Questo caso dimostra **l'elevata qualità del database di reputazione IP della soluzione Flowmon**.

botnet

(Finance)

Flowmon
Driving Network Visibility

Sicurezza

Attacchi e distribuzione di SPAM

Flowmon
Driving Network Visibility

Massiccio cyber attack

Un fornitore di connettività dati lancia il sistema Flowmon con l'obiettivo di segnalare gli attacchi e gli incidenti ai propri clienti, che utilizzano tale connettività Internet.

La soluzione, ad esempio, ha rilevato presso un grossa catena di rivendita di pneumatici**, una stazione infetta che inizialmente eseguiva una scansione orizzontale del servizio RDP** sull'estensione IP della Romania e **successivamente avviava un massiccio attacco di dizionario** sulle stazioni che hanno reagito alla scansione iniziale.

Attack

(Internet services)

Flowmon
Driving Network Visibility

Fonte di distribuzione SPAM

Il nostro fornitore di connettività Internet ci ha avvertito **sulla distribuzione di SPAM dalla nostra rete**.

In parte ne eravamo a conoscenza attraverso una comunicazione di ‘avvertimento’ su **limiti del servizio del** nostro indirizzo IP pubblico come fonte di posta indesiderata.

Poiché utilizziamo il NAT come la maggior parte delle società, **non siamo stati in grado di rilevare la fonte SPAM**.

Abbiamo acquistato la soluzione Flowmon ed eseguito l'analisi.

La stazione infetta è stata rilevata immediatamente in base alla maggiore quantità di connessioni al server di posta del provider.

In seguito, fortunatamente, non abbiamo dovuto affrontare i limiti del servizio.

Spam (Non-government non-profit organization)

Security

Applicazioni indesiderate, perdita di dati e comportamento degli utenti

Flowmon
Driving Network Visibility

P2P networks

- Abbiamo scoperto **diversi utenti** che **hanno utilizzato** la nostra rete aziendale per il **servizio Bittorent.**

Oggi, la soluzione Flowmon **ci avvisa immediatamente** in caso di eventi simili.

Monitoriamo **un vero declino degli incidenti** nel tempo poiché i **nostri utenti già** sanno che abbiamo il pieno controllo della nostra rete.

applicazioni indesiderate

(Food industry)

Falso DHCP server

- A volte si verifica che un dipendente porta il proprio dispositivo e tenta di collegarlo alla rete (per non parlare dei consulenti).

I maggiori problemi sono causati dai dispositivi con il servizio server DHCP.

Grazie a Flowmon ADS oggi identifichiamo immadiatamente un falso server DHCP nella nostra rete, una volta invece ci mettevamo troppo tempo.

comportamento utente

(Healthcare)

Perdita dati

- La soluzione Flowmon ha rilevato **un caricamento sospetto di dati** dalla nostra rete in un repository di dati pubblici. Erano **centinaia di MB di dati.**

Una **stazione nella nostra rete locale** è stata identificata come fonte.

Abbiamo scoperto che **uno dei dipendenti**, che aveva **rescisso il contratto** con la società, desiderava eseguire un **backup dei dati aziendali** x future necessità.

(Law and tax agency)

perdita di dati

Flowmon Networks

is an international vendor devoted to innovative network traffic & performance & security monitoring

1000+ customers 40 countries

First 100G probes in the world

Strong R&D background

European origin

Customer references

SEGA, AVG, KBC, Konica Minolta, Vodafone, TDK, Oriflame Sweden, Siemens, Slovenská sporiteľňa, Volkswagen, orange, Telefónica, Allianz, hp, T-Mobile, GÉANT Networks • Services • People, KIA, upc, Raiffeisen BANK, e·on

Flowmon Driving Network Visibility

Technology partner of premium vendors

IBM

vmware

Check Point SOFTWARE TECHNOLOGIES LTD.

f5

ixia

Gigamon

radware

A10

The only vendor recognized in both NetFlow related Gartner reports – network visibility & security

Gartner MAGIC QUADRANT

50™ Technology Fast 50 Deloitte.

RED HERRING EUROPE WINNER 100

Flowmon
Driving Network Visibility

Thank you

Performance monitoring, visibility and security with a single solution

Angelo Sbardellini

Angelo.sbardellini@Flowmon.com

Flowmon Networks a.s.
Sochorova 3232/34
616 00 Brno, Czech Republic
www.flowmon.com

Flowmon
Driving Network Visibility