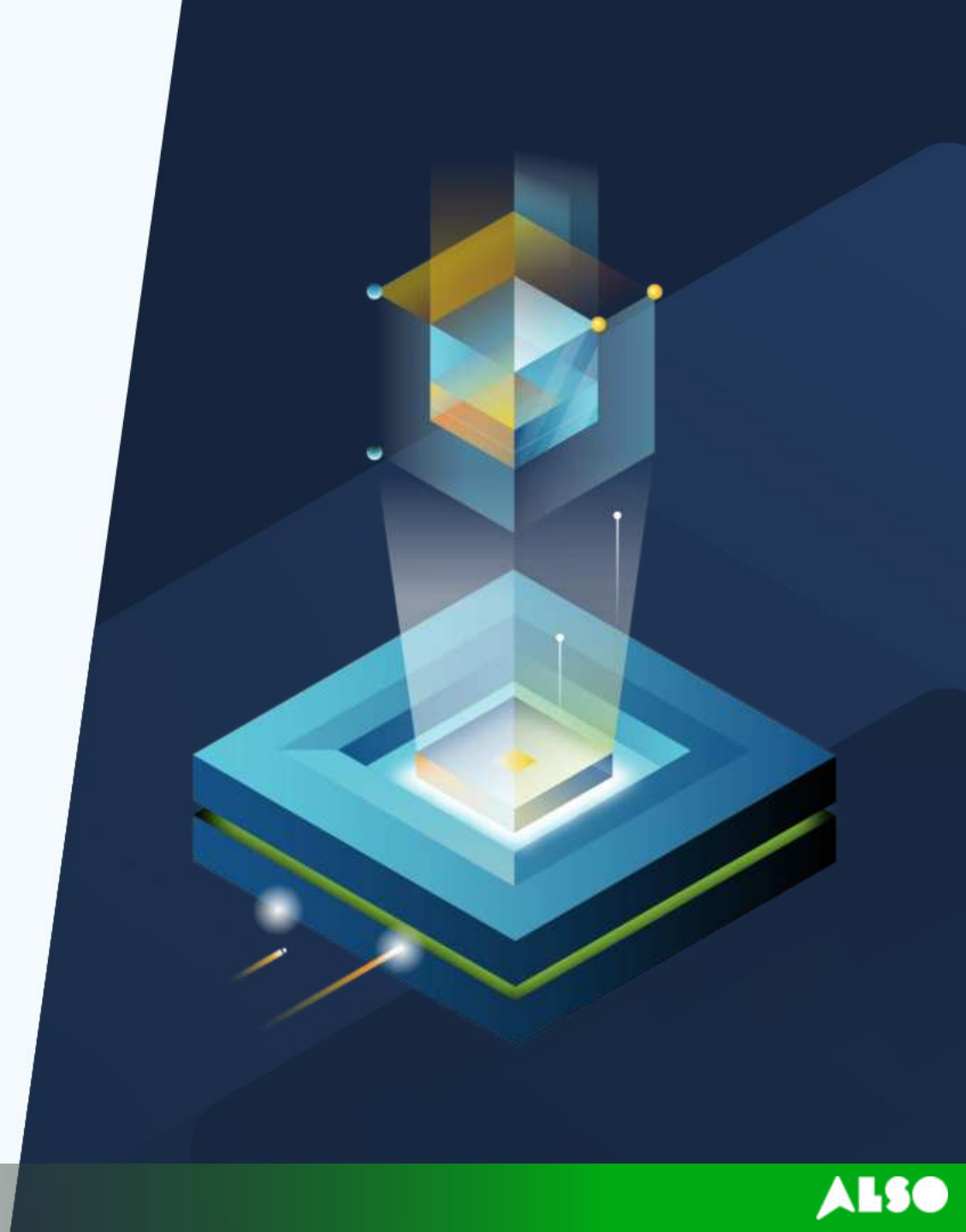
Progress® | Flowmon

KĀ IEGŪT PILNU TĪKLA REDZAMĪBU AR TĪKLA VEIKTSPĒJAS UN UZRAUDZĪBAS RISINĀJUMU



Izaicinājumi - ..un kur ir problēma?

Tīklā?

Serverī?

Lietotājā?

90%

10%

Problēmu risināšanas laiks tiek tērēts, mēģinot noskaidrot, vai problēma patiešām pastāv un kur?!

Novēršana

Vai mēs varam būt proaktīvi – ne tikai reaktīvi reaģēt uz incidentiem!?

Kāpēc mums būtu nepieciešams šāds risinājums?

Tāpēc, ka iegūt pilnu tīkla redzamību ir pamata – darbības nepārtrauktības un drošības faktors

Kā atrisināt tīkla, aplikāciju un drošības problēmas?

Zināt..

Ka aplikācijas un tīkla resursi ir nepārtraukti pieejami un droši

Iegūt..

Visas nepieciešamās tīkla paketes, telemetrijas datus, datu plūsmas pilnvērtīgai incidenta izmeklēšanai

Uzraudzīt..

Nepārtraukti visu tīkla datu plūsmu un aplikāciju darbību – anomālijas

Aizsargāt..

Organizāciju no iespējamajiem drošības riskiem

Viens no risinājumiem - Flowmon

Progress®
Flowmon®

Portfolio – pieejamie moduļi

Network Detection and Response & Anomaly

(NDR/ADS)

Nodrošina uz AI – mākslīgā intelekta un tīkla darbības paternu balstītu anomālija un uzbrukumu identificēšanu. Pirms tie nodara kaitējumu Jūsu Organizācijai.
(IPS funkcionalitāte)

Network Performance Monitoring & Diagnostics

(NPMD)

Inteliģenta tīkla datu plūsmas (FLOW) ieguve – tīkla datu plūsmas rādītāju uzraudzība un automatizēta problēmu analīze

Application Performance Monitoring

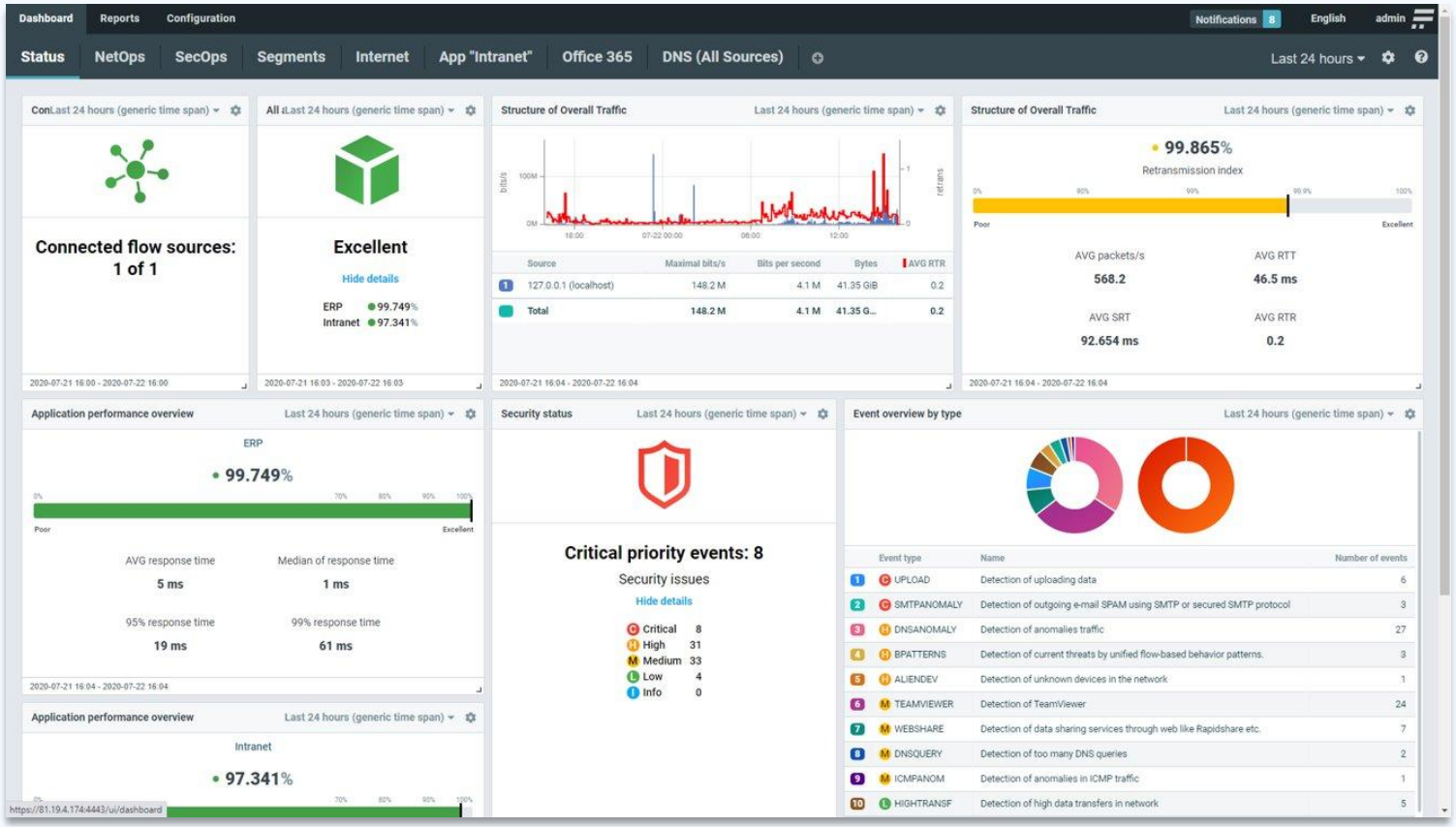
(APM)

Ieskatu aplikāciju un datubāzu darbībā. To nepārtraukta uzraudzība un problēmu identificēšana.

Packet Investigator

Tīkla pakešu analizators

Flowmon nodrošina vairāku līmeņu redzamību



- Viens risinājums visas infrastruktūras monitorēšanai
- Reālā laika veiktspējas izmaiņas
- Izmantošanas, lietojuma un jaudas monitorēšana
- Vājo punktu (Bottleneck) kļūdu noteikšanas, analizēšana – ieteikumi.

2 pieejas tīkla uzraudzībai - Full Packet vs. Flow Data

Full packet

Detalizētāks ieskats tīkla datu paketēs un incidentu izmeklēšanā

Datu uzglabāšana var būt izaicinājums un dārga

Neefektīva šifrētu datu plūsmas analīze

Flow Data

Darbojas augstas veiktspējas tīkla infrastruktūrās

Var analizēt šifrētu datu plūsmu

L7 nodrošina 95% pārklājumu

Atsevišķos gadījumos var pietrūkt detalizācija

Packet	1 min 75 GB	1 hour 4.5 TB	1 day 108 TB
Flow	1 min 150 MB	1 hour 9 GB	1 day 216 GB

Storage required for 10Gbps traffic

Progress Flowmon Arhitektūra

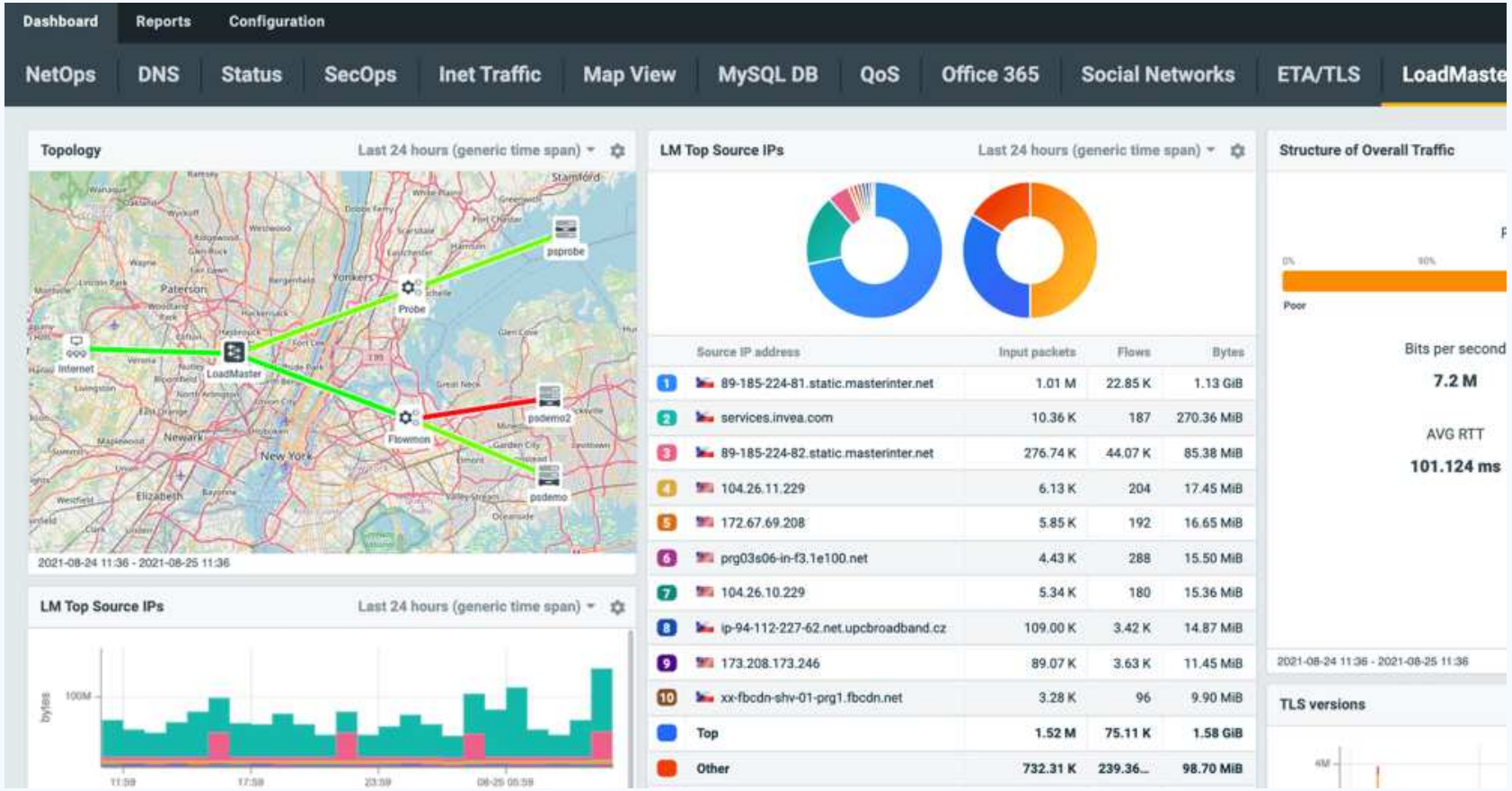
- Flowmon Collector (Datu analizators)
- Flowmon Probe (Sensors)

Virtuāla instalācija / Fiziska iekārta

Flowmon Collector (Datu analizators)

NetFlow Collector ir atsevišķa ierīce (fiziska vai virtuāla) datu plūsmas datu savākšanai, ilgstošai glabāšanai un analīzei no ierīcēm - slodzes dalītāji, komutatori, maršrutētāji un ugunsmūriem), No Probes sensoriem, specializētiem sensoriem (NetworktTap) un citiem plūsmas avotiem. Collector nodrošina datu vizualizāciju.

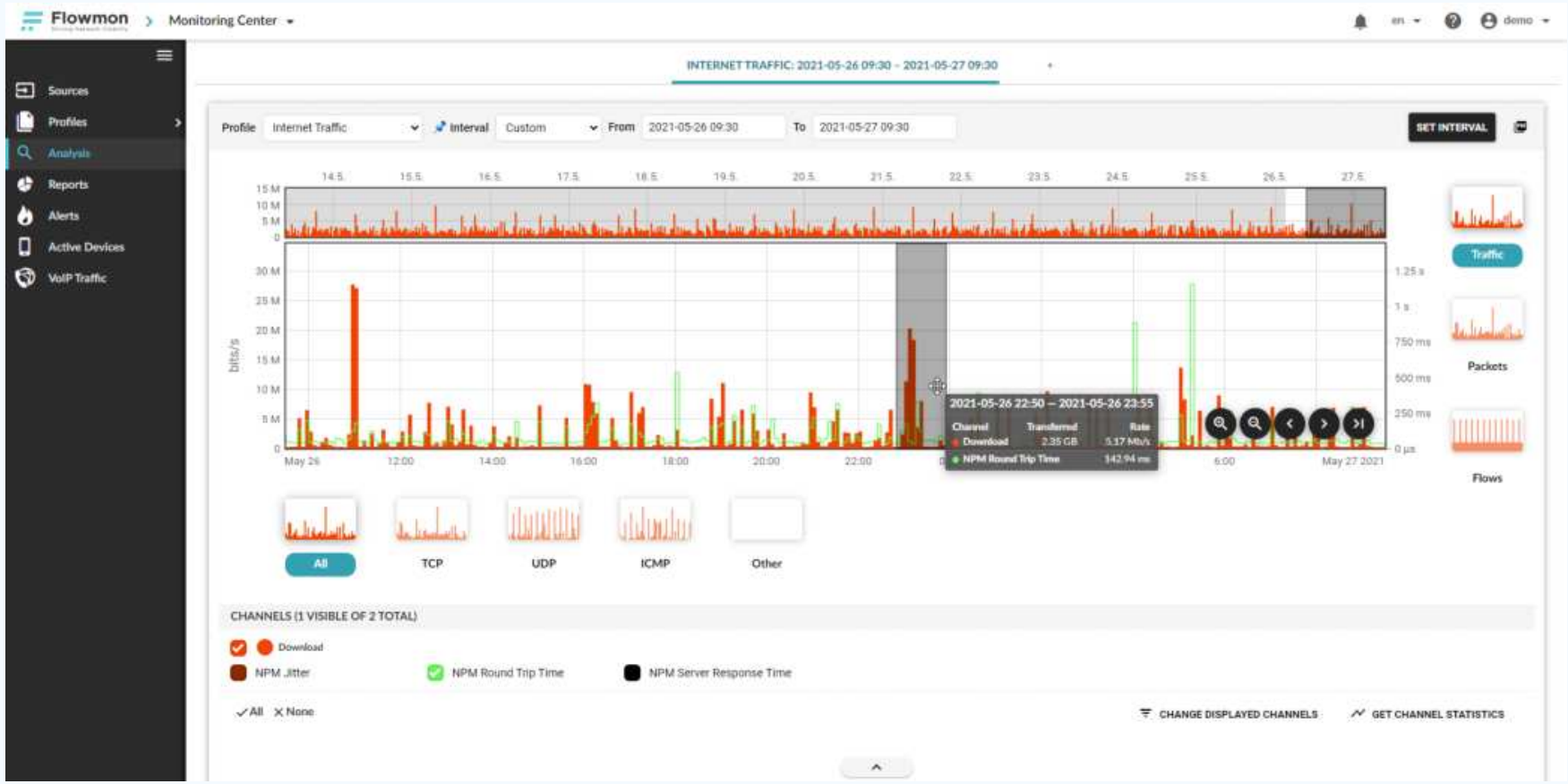
- Pielāgojami logrīki un cilnes.
- Dažādas pieejas / dažādām lomām.



Flowmon Collector (Datu analizators)

Problēmu novēršana un izmeklēšana

Collector – Ne tikai pārrauga sarkano/zaļo statusu – pēc izveidotajām politikām. Bet arī izseko analizē atsevišķu lietotāju mijiedarbību ar lietojumprogrammām, lai sniegtu pilnīgu izpratni par visu digitālo vidi. Šī pieeja ļauj nekavējoties noteikt to problēmu galveno cēloni, kas ietekmē lietotājus un pakalpojumus, un veikt koriģējošus pasākumus.



Flowmon Collector (Datu analizators)

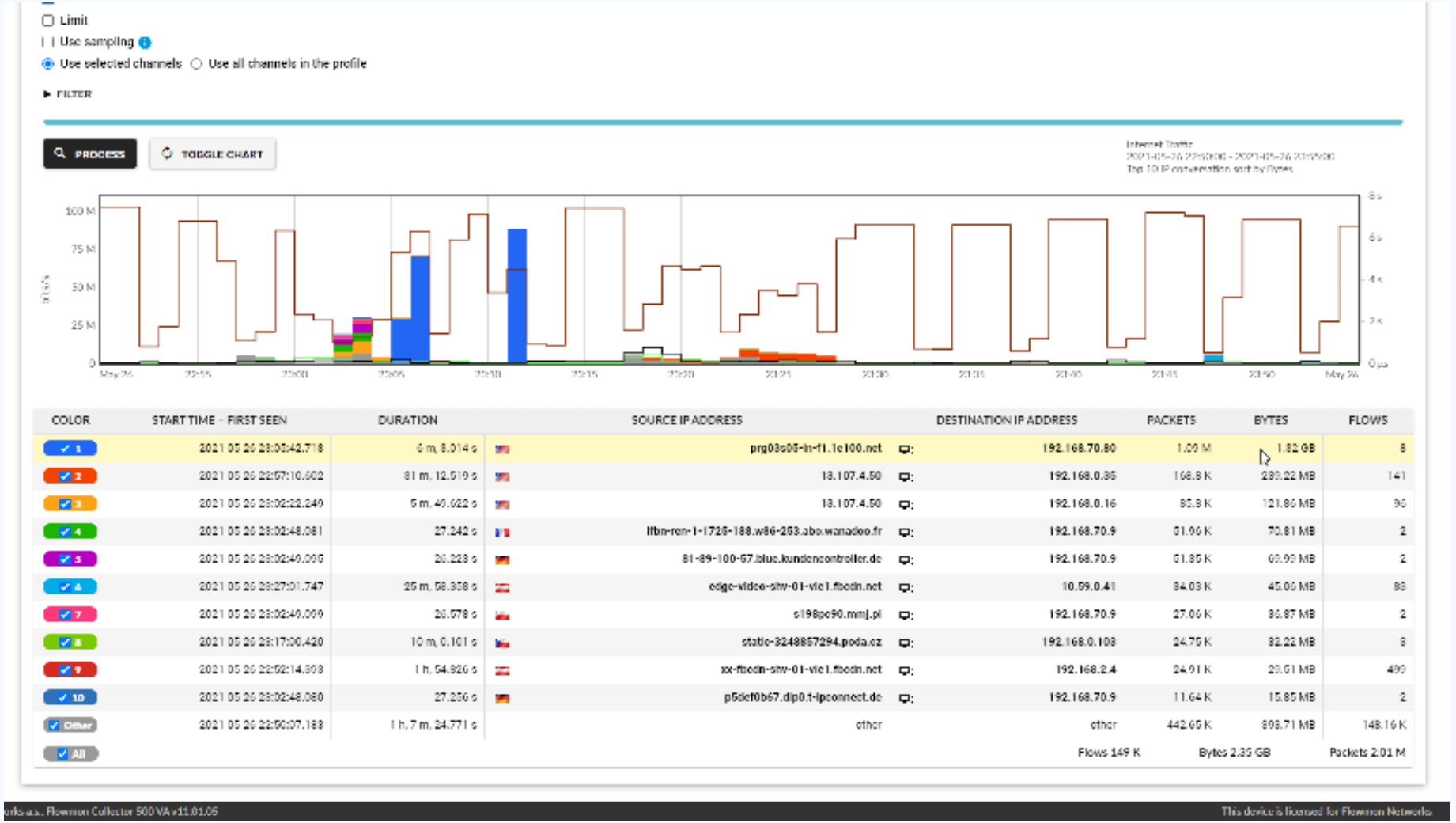
Cloud and SaaS monitoring

Flowmon izmanto pasīvos tīkla sensorus, kas ir pieejami kā virtuālas ierīces privātajā un publiskajā mākonī, un tiem var piekļūt no attiecīgās vietas, lai pārbaudītu visu trafiku attiecībā uz lietojumprogrammām saistītu saziņu. Collector izseko mijiedarbību starp lietotājiem un lietojumprogrammām, lai identificētu vājās vietas jebkurā lietojumprogrammu ķēdē.

Flowmon Collector (Datu analizators)

Analytics drilldown

Izpētes opcijas ir pieejamas jebkurā informācijas paneļa vietā. Katru logrīku var parādīt analītiskā skatā, lai iegūtu pilnu informāciju, līdz pat plūsmu vai pakešu līmenim. Ir iespējas filtrēt pēc protokoliem, laika periodiem, avota/galamērķa IP adreses, lietotāji, aplikācijas u.c.



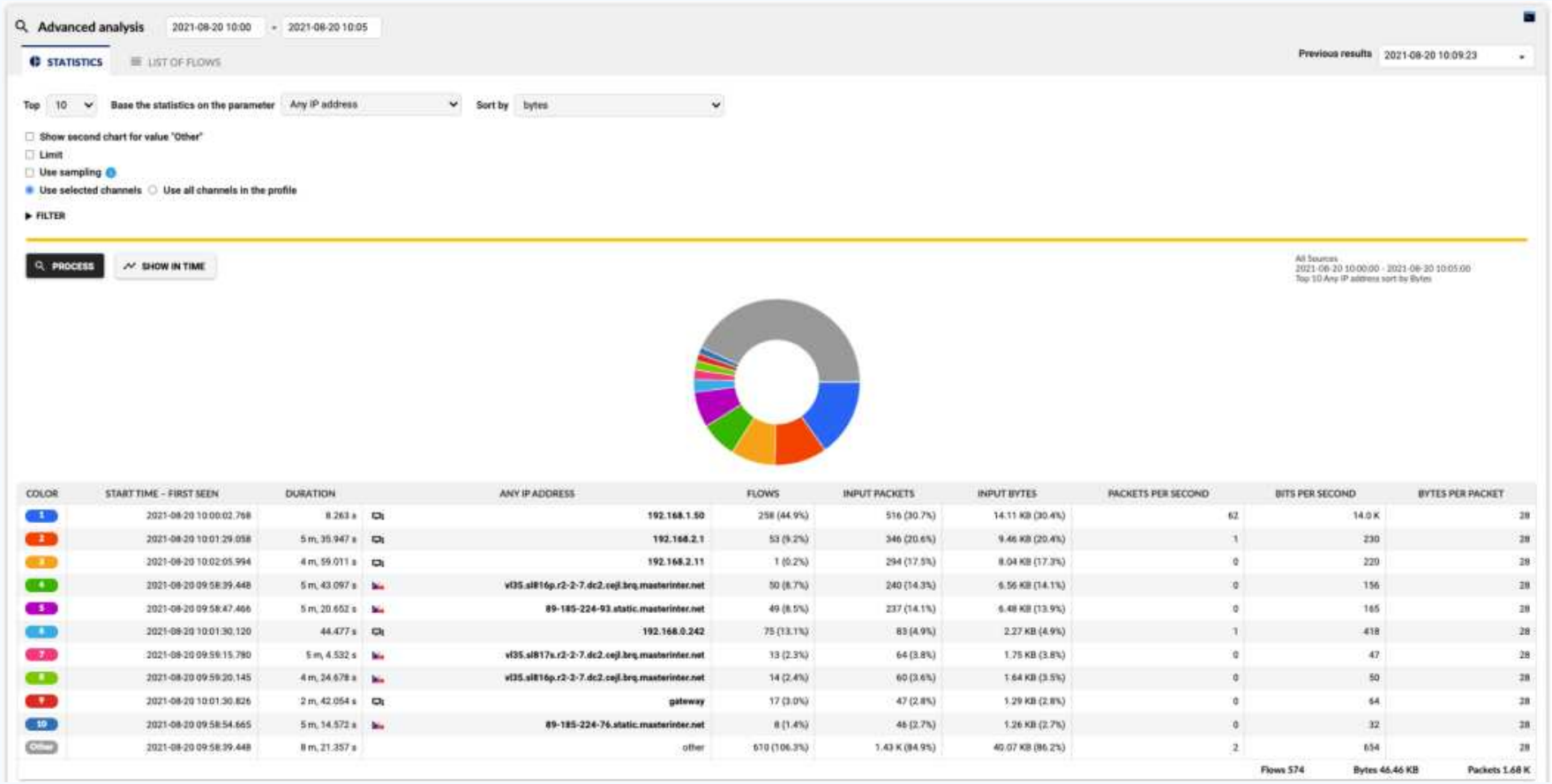
Flowmon Probe (Sensors)

Flowmon Probe ir tīkla datu plūsmas datu ieguves sensors (fizisks/virtuāls), kas ģenerē datus līdz pat lietojumprogrammas līmenim un mēra veiktspēju. – Tālāk nododot datus analīzei un attēlošanai uz kolektoru (Collector.)

Use it anywhere
Hardware, virtual or cloud, from 10 Mb/s to 100 Gb/s.

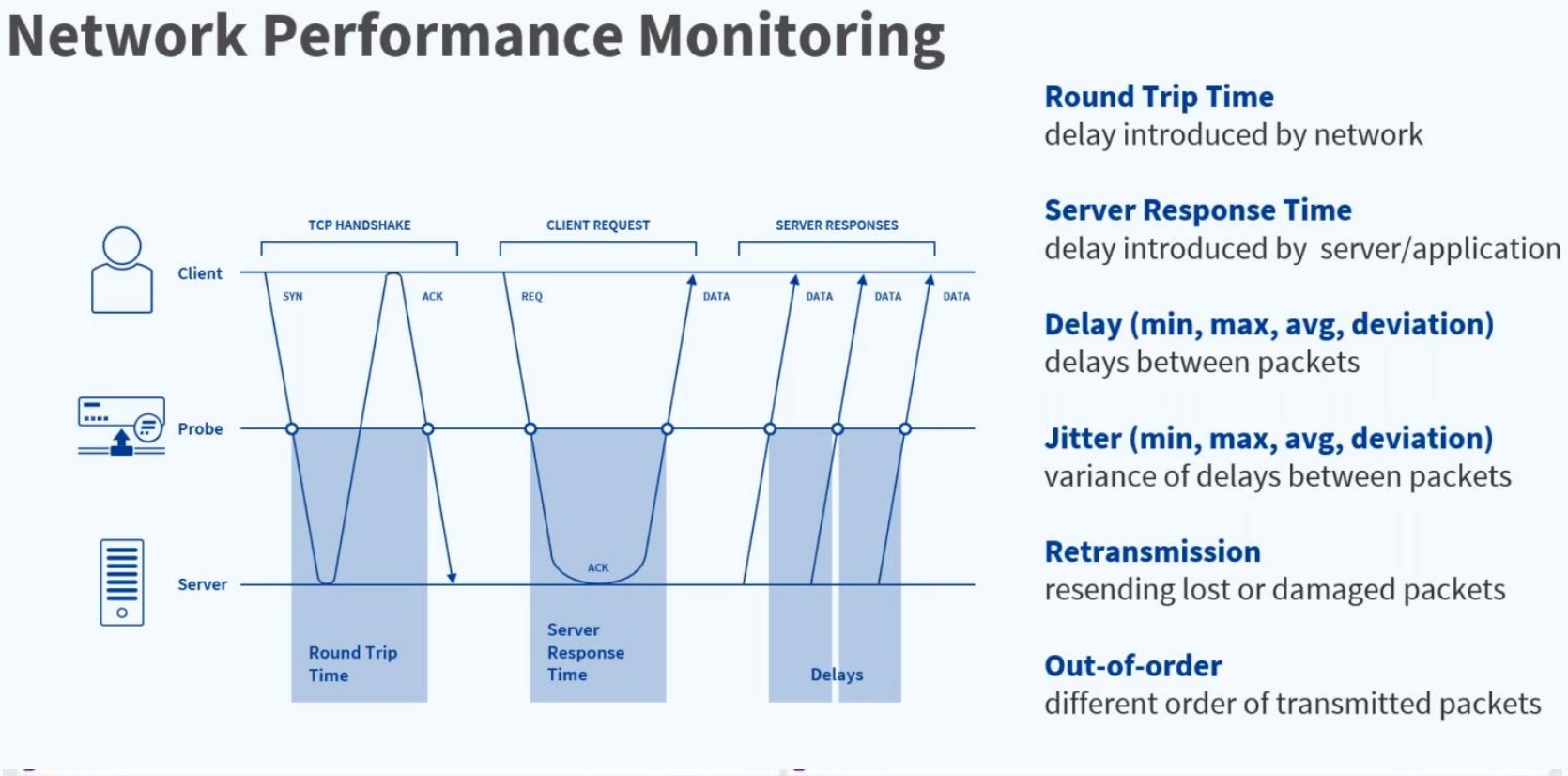
Stay non-intrusive
The Probe connects passively through a SPAN port or network TAP.

Network data is pre-filtered to enable clearer analysis and visualization.



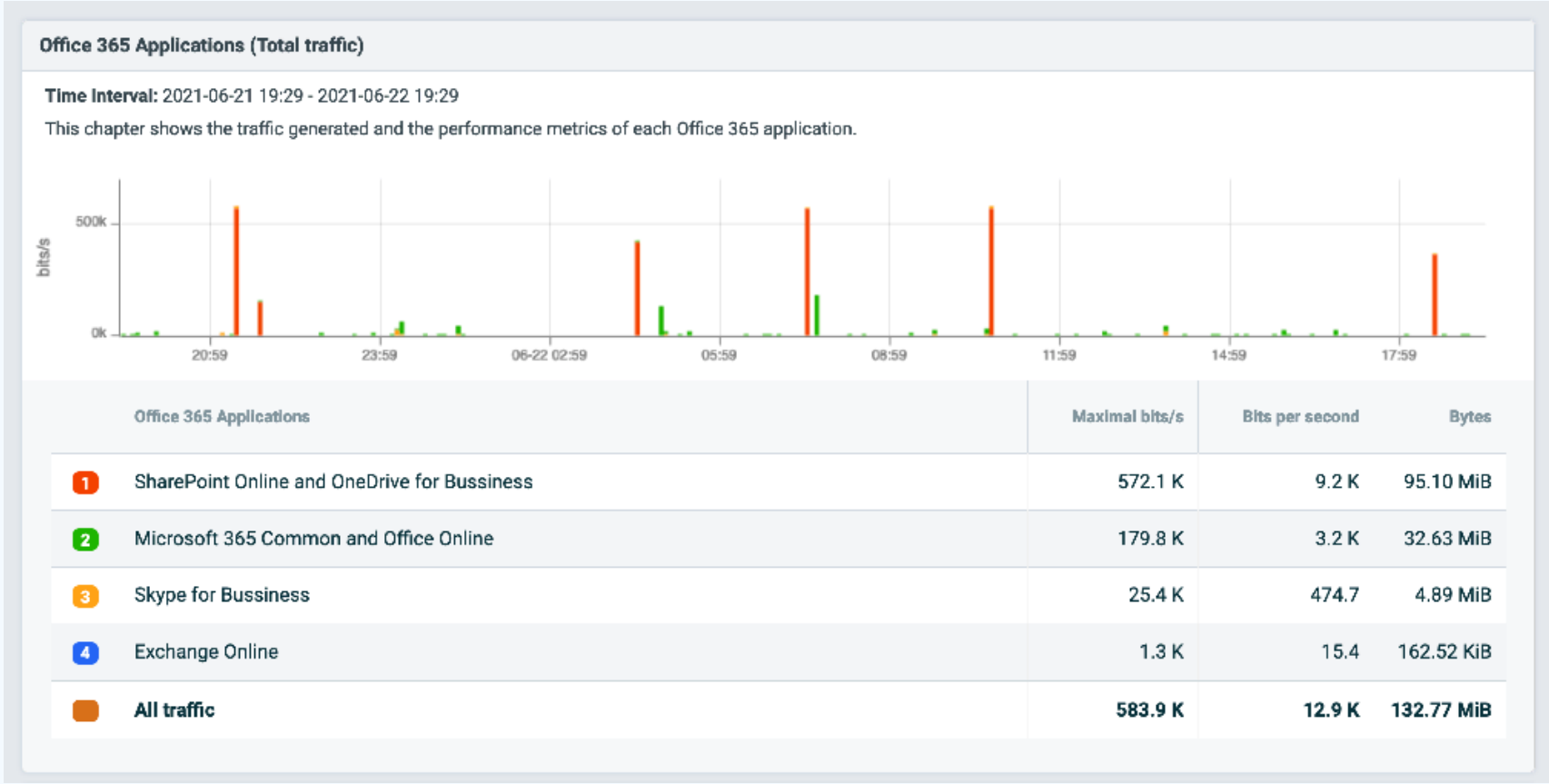
Flowmon Probe (Sensors)

Redzamība L2, L3/4, L7
Sensori sākotnēji apkopo L2–L4 informāciju par IP adresēm, protokoliem, servera reakcijas laiku, Roundtrip, jitter u.c, vienlaikus uzrauga reālo lietotāja un lietojumprogrammas sasaisti. Turklāt Flowmon IPFIX paplašinājums nodrošina papildu L7 datus, piemēram, resursdatora nosaukumus, URL, pārlūkprogrammas informāciju HTTP/S protokoliem un citus laukus tādiem protokoliem kā DNS, DHCP, SQL, SMTP vai Samba/CIFS un citus. atpazīšanas (NBAR2).



Flowmon Probe (Sensors)

Lietojumprogrammu atpazīšana
Flowmon ziņo par lietojumprogrammu izmantošanu, analizējot L7 paketes un eksportējot uz tīkla balstītas lietojumprogrammu atpazīšanas (NBAR2) nosaukumu vai sniedz informāciju par tīkla trafika avotu vai galamērķi.

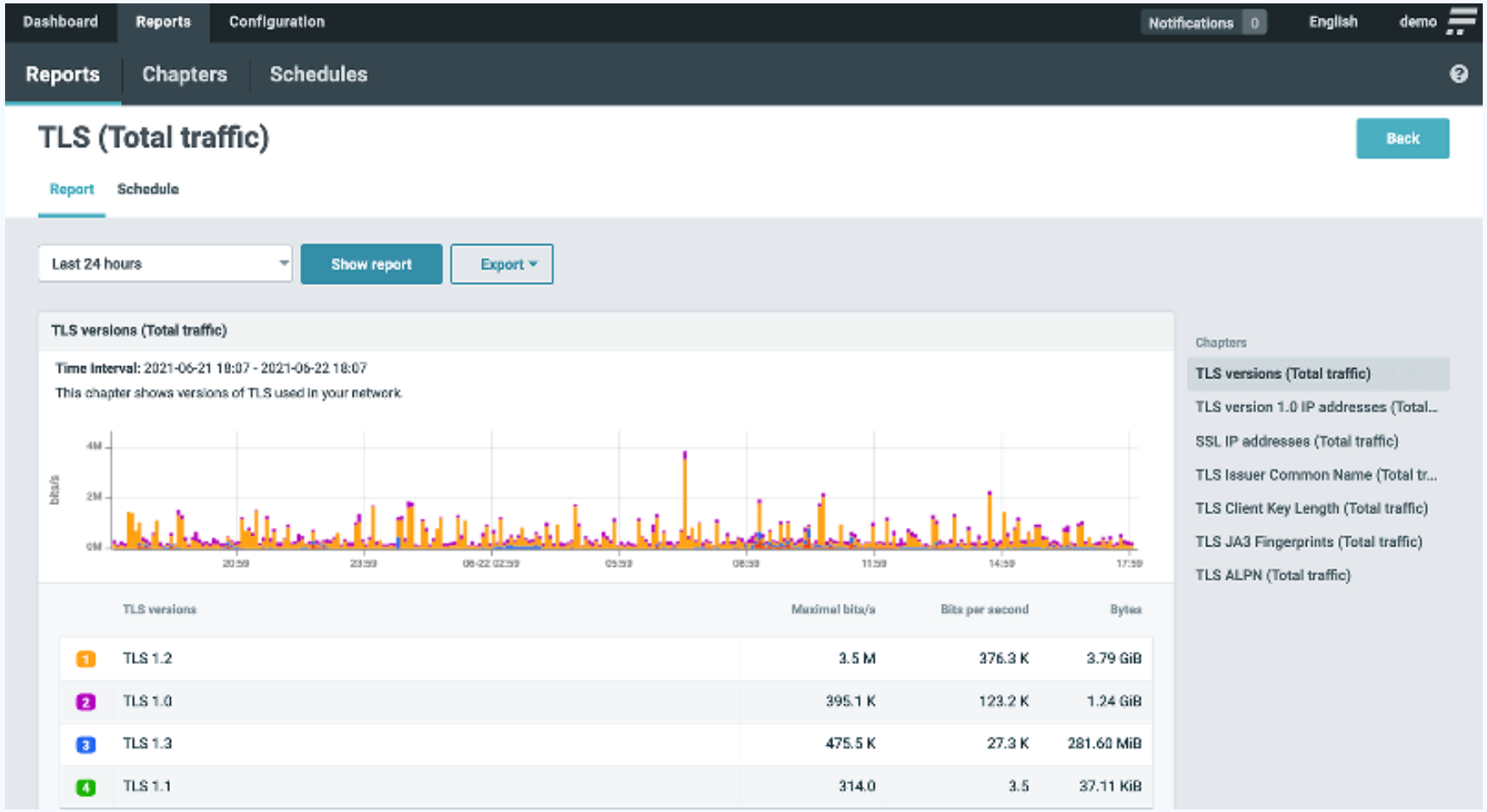


	Office 365 Applications	Maximal bits/s	Bits per second	Bytes
1	SharePoint Online and OneDrive for Bussiness	572.1 K	9.2 K	95.10 MiB
2	Microsoft 365 Common and Office Online	179.8 K	3.2 K	32.63 MiB
3	Skype for Bussiness	25.4 K	474.7	4.89 MiB
4	Exchange Online	1.3 K	15.4	162.52 KiB
	All traffic	**583.9 K**	**12.9 K**	**132.77 MiB**

Flowmon Probe (Sensors)

Šifrēta trafika analīze

Flowmon šifrēta tīkla datu plūsmas analīze apkopo tīkla trafika metadatus IPFIX formātā, izmantojot sensorus, un bagātina tos ar TLS protokola informāciju. Tas nodrošina daudz informācijas par trafiku un ļauj identificēt novecojušus SSL sertifikātus, politikām neatbilstošus sertifikātus, šifrēšanas stiprumu un vecās TLS versijas, kurās var būt kļūdas vai ievainojamības.

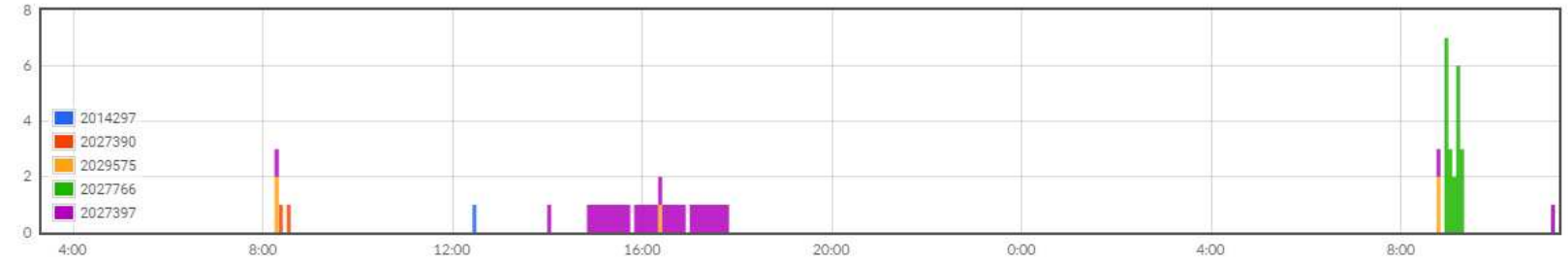


Flowmon Probe (Sensors)

Flowmon IDS (By Suricata)
Tiek nodrošināta pakešu pārbaude, lai meklētu iespējamo ielaušanos, drošības incidentus - papildinot Flowmon ADS drošības līmeni. Darbojas vidēs ar jebkuru saites ātrumu no 1 Gb/s līdz 100 Gb/s.

IDS event browser

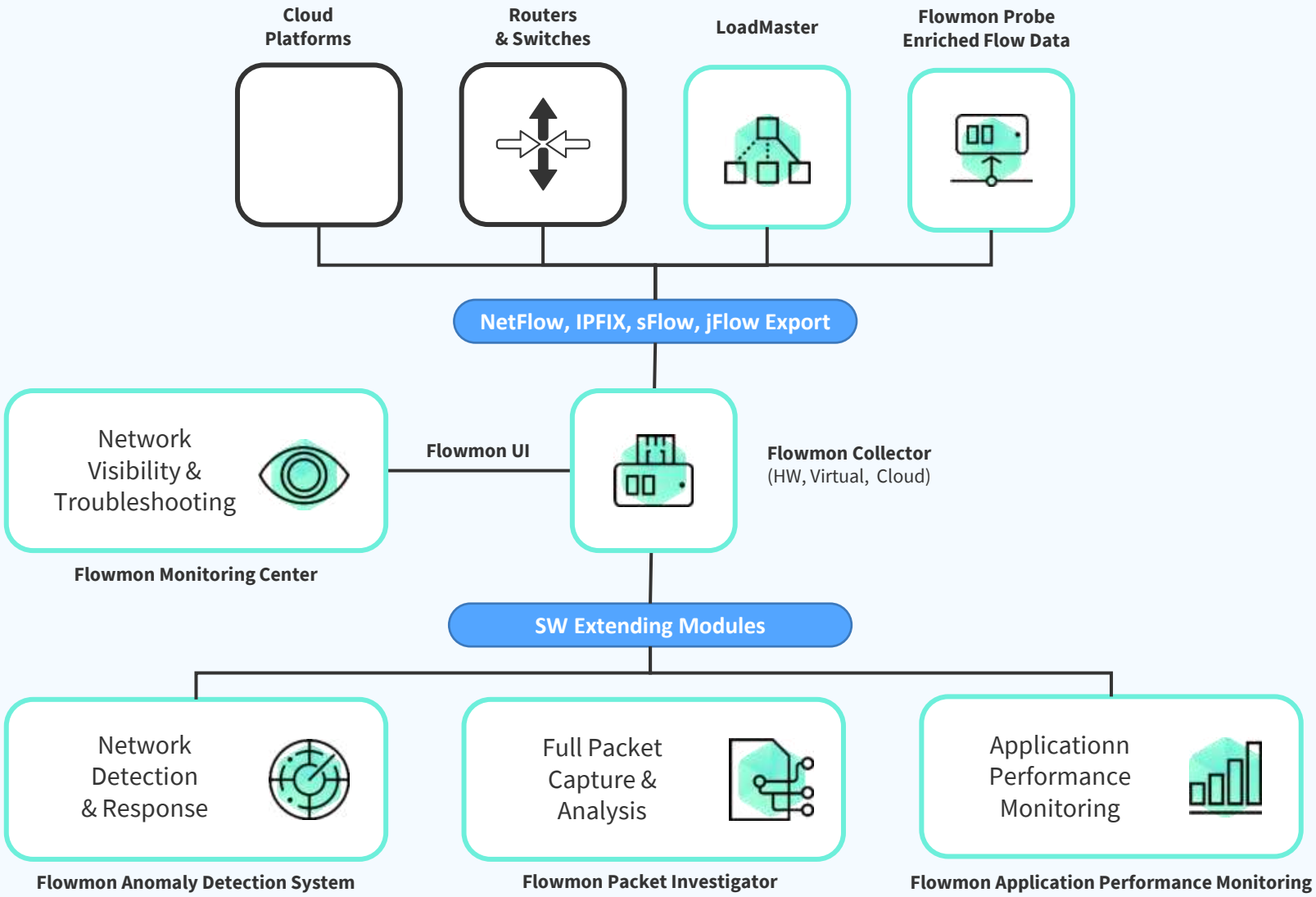
From 2021-06-16 03:20 To 2021-06-17 11:20 Source IP 192.168.0.88 Target IP Limit 100 SEARCH



	FIRST SEEN	LAST SEEN	SOURCE IP (BASE FOR AGGREGATION)	SOURCE PORT	DESTINATION IP (BASE FOR AGGREGATION)	DESTINATION PORT	SIGNATURE ID (BASE FOR AGGREGATION)	SIGNATURE (BASE FOR AGGREGATION)	LOG SOURCE IP	LOG SOURCE INTERFACE	SOURCE USER IDENTITY	DESTINATION USER IDENTITY	COUNT	OTHER INFO
>	2021-06-16 08:18:42	2021-06-17 11:14:28	192.168.0.88	57621	192.168.0.255	57621	2027397	ET POLICY Spotify P2P Client	127.0.0.1	idsp_eth2_out	PC_RECEPCE		38	**category:** Not Suspicious Traffic | **severity:** 3 | **action:** allowed | **groupID:** 1 | **rev:** 1
>	2021-06-16 08:19:09	2021-06-16 08:19:17	192.168.0.88	63579	5.62	80	2029575	ET POLICY External IP Lookup (avast .com)	127.0.0.1	idsp_eth2_out	PC_RECEPCE		2	**category:** Potential Corporate Privacy Violation | **severity:** 1 | **action:** allowed | **groupID:** 1 | **rev:** 2
>	2021-06-16 08:22:35	2021-06-16 08:22:35	192.168.0.88	58284	52.247.	80	2027390	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	127.0.0.1	idsp_eth2_out	PC_RECEPCE		1	**category:** Unknown Traffic | **severity:** 3 | **action:** allowed | **groupID:** 1 | **rev:** 2
>	2021-06-16 08:31:51	2021-06-16 08:31:51	192.168.0.88	58281	184.24.	80	2027390	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	127.0.0.1	N/A	PC_RECEPCE		1	**category:** Unknown Traffic | **severity:** 3 | **action:** allowed | **groupID:** 1 | **rev:** 2
>	2021-06-16 12:25:00	2021-06-16 12:25:00	192.168.0.88	49627	137.254.	80	2014297	ET POLICY Vulnerable Java Version 1.7.x Detected	127.0.0.1	idsp_eth2_out	PC_RECEPCE		1	**category:** Potentially Bad Traffic | **severity:** 2 | **action:** allowed | **groupID:** 1 | **rev:** 60

Suricata is a high performance, open source network analysis and threat detection software used by most private and public organizations, and embedded by major vendors to protect their assets.

Progress Flowmon Arhitektūra



aws

Microsoft Hyper-V

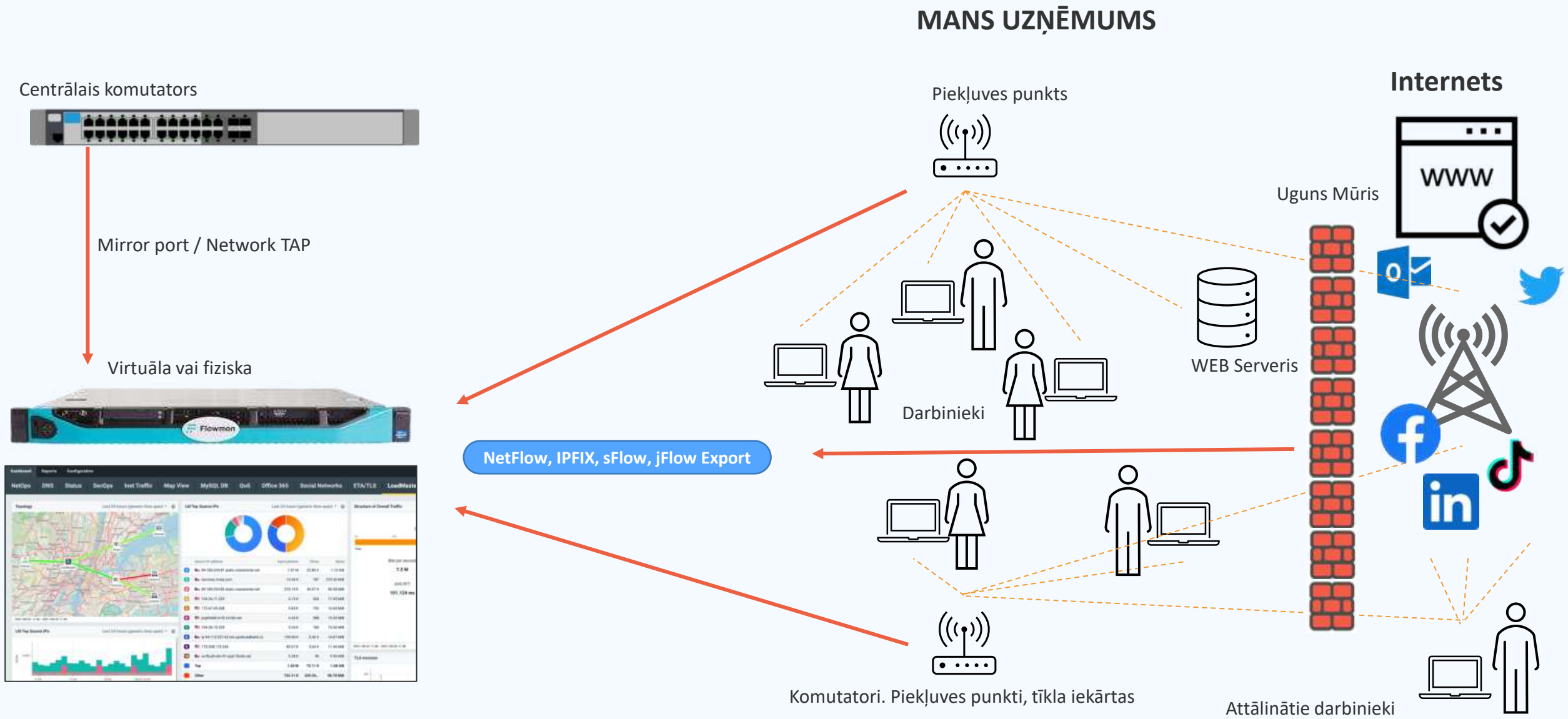
Microsoft Azure

Google Cloud Platform

vmware

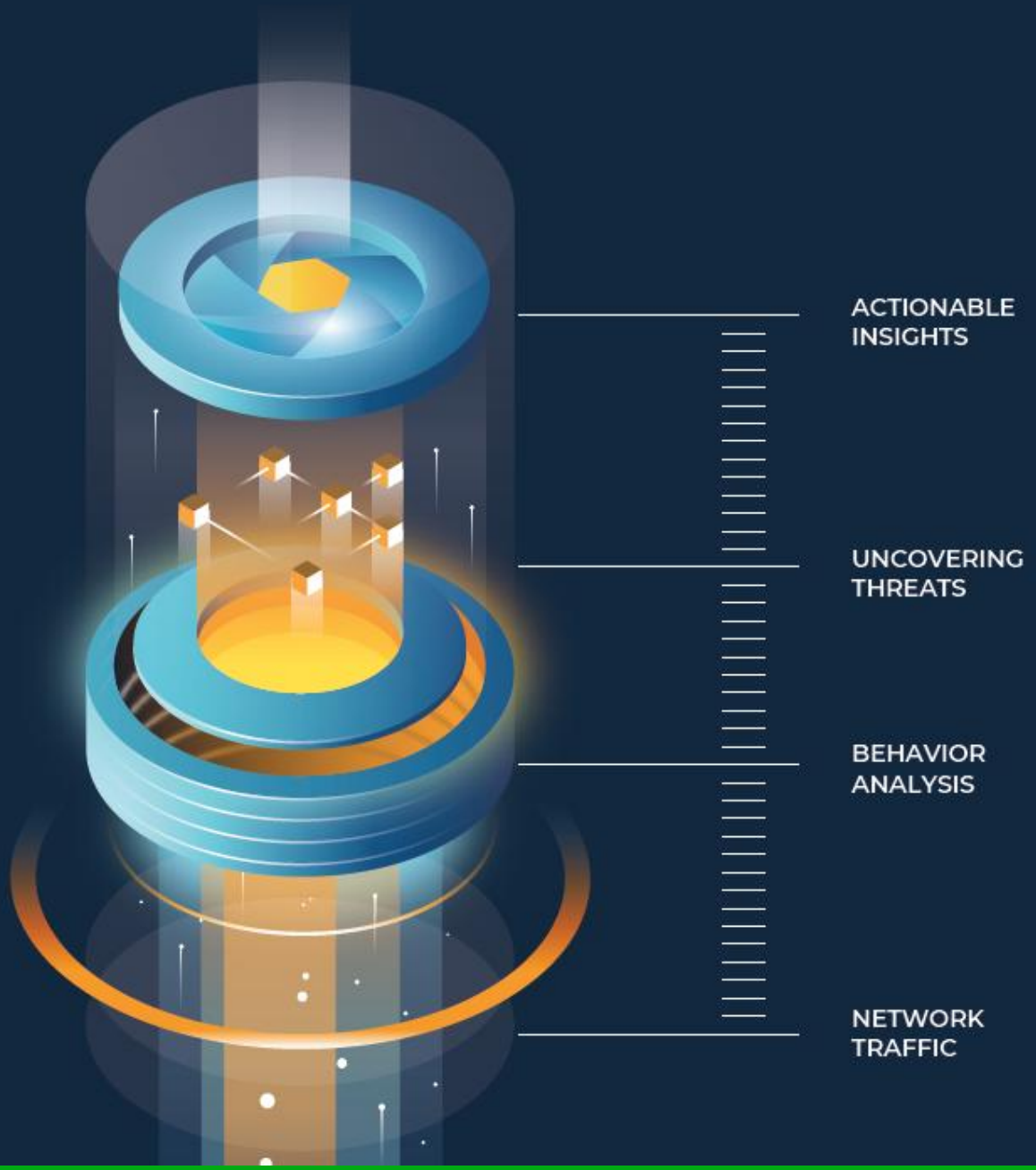
KVM

Progress Flowmon Arhitektūra



Progress® | Flowmon

Anomaly Detection System



ALSO

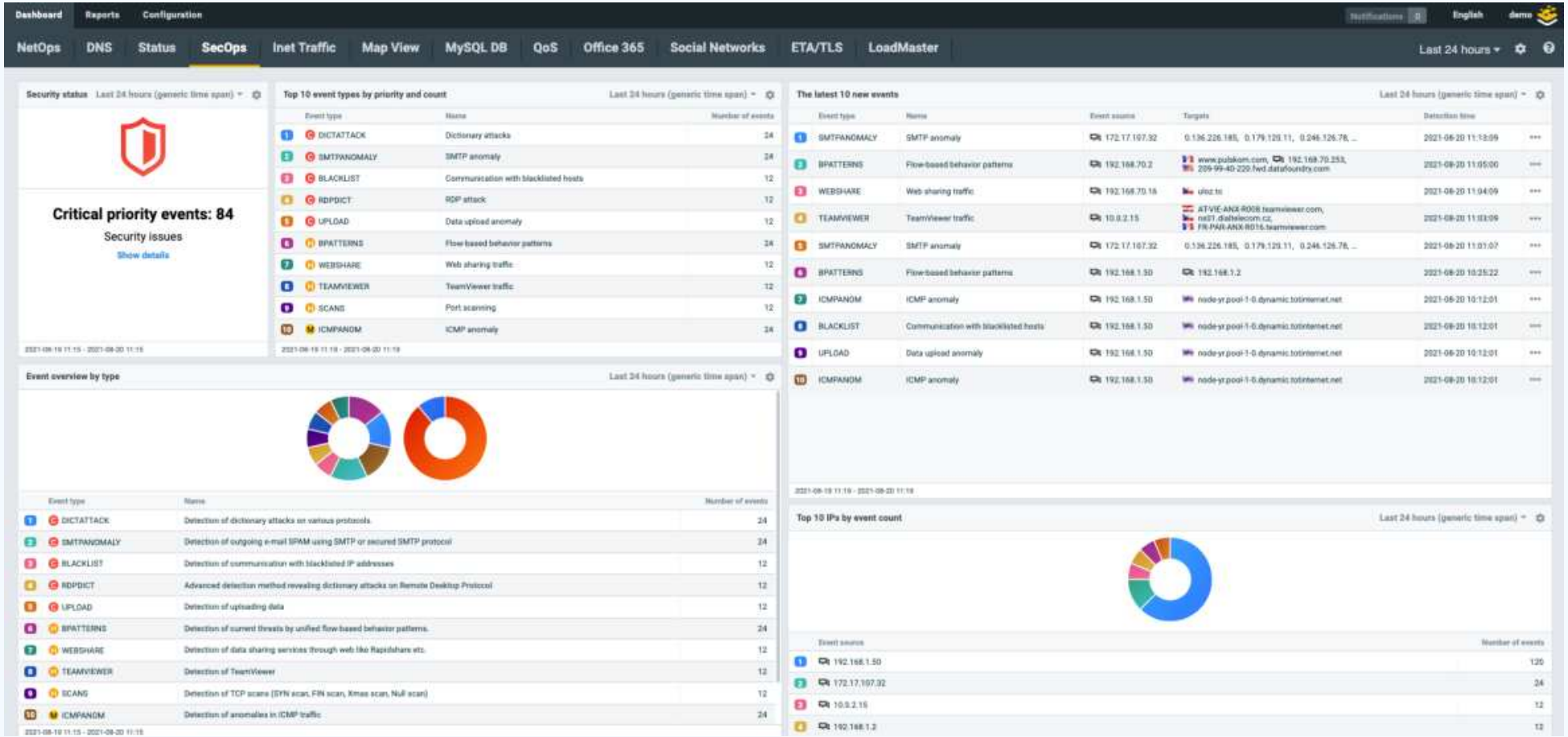
Tīkla anomāliju detektēšana (ADS)

Flowmon ADS izmanto uzvedības analīzes algoritmus, lai atklātu anomālijas, kas slēptas tīkla datu plūsmā, lai atklātu ļaunprātīgu uzvedību, ļaunatūru (Datora virusu darbību), uzbrukumus infrastruktūras kritiskām lietojumprogrammām un datu pārkāpumus.

Nodrošina redzamību starp perimetra un gala iekārtu aizsardzības

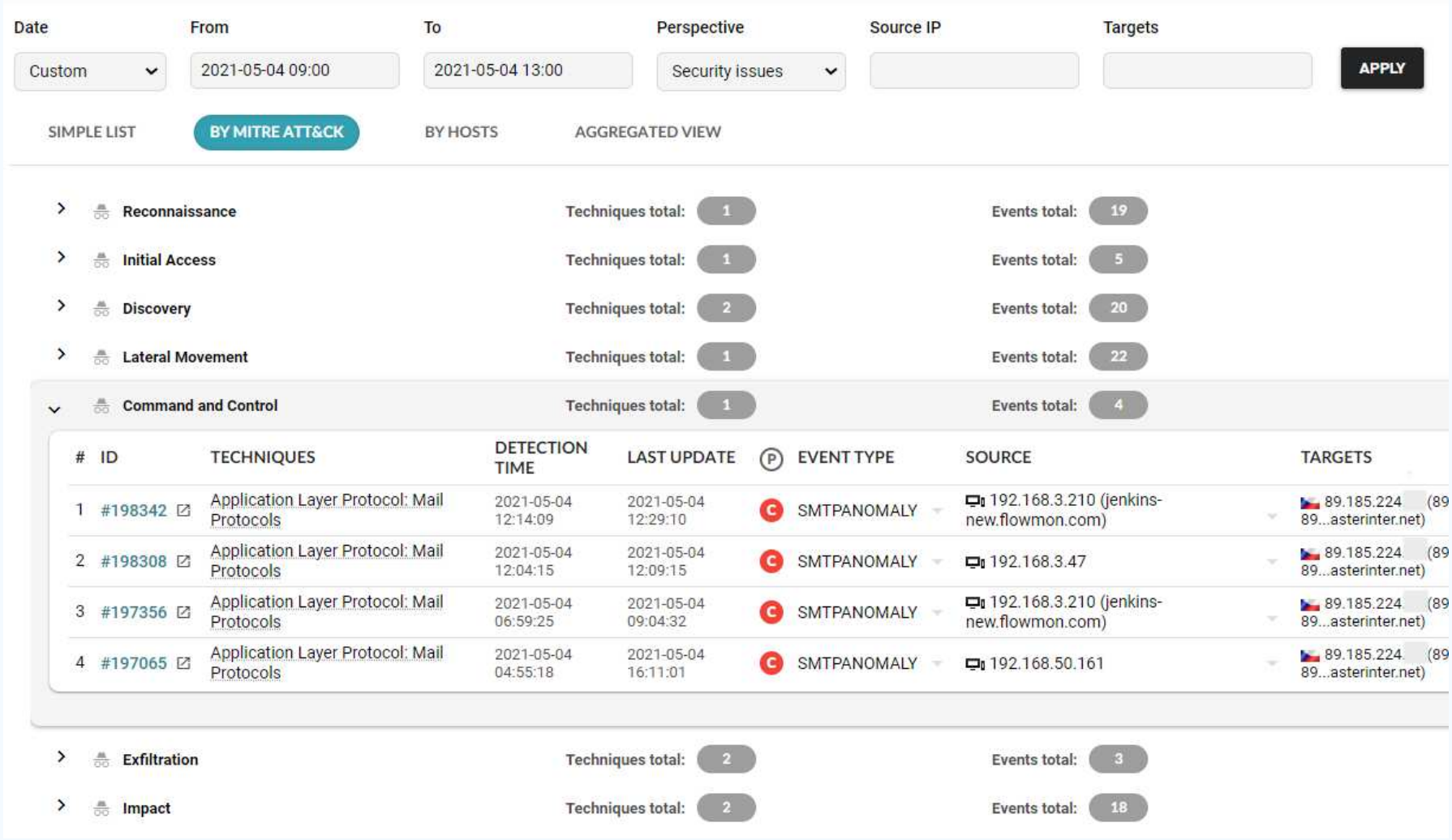
Palīdz atklāt dažāda veida uzbrukumus (ielaušanās, ļaunatūru, dažādus iekšējos un ārējos draudus).

Izmanto mašīnmācīšanos, lai atklātu nultās dienas draudus.



(ADS)

Katra uzbrukuma posma analīze
Flowmon ADS pievieno jūsu drošības matricai uz tīklu orientētu aizsardzības slāni (skatiet sadaļu SOC Visibility Triad), lai atklātu tīkla anomālijas, kas norāda uz nezināmu un iekšēju apdraudējumu darbību, kuru parasti nevar noteikt ar perimetra un lokālo datoru aizsardzības risinājumiem. Flowmon veic incidentu vizualizāciju atbilstoši MITRE ATT&CK® ietvaram - sniedz informāciju par pārkāpuma apjomu, nopietnību un turpmāko attīstību.

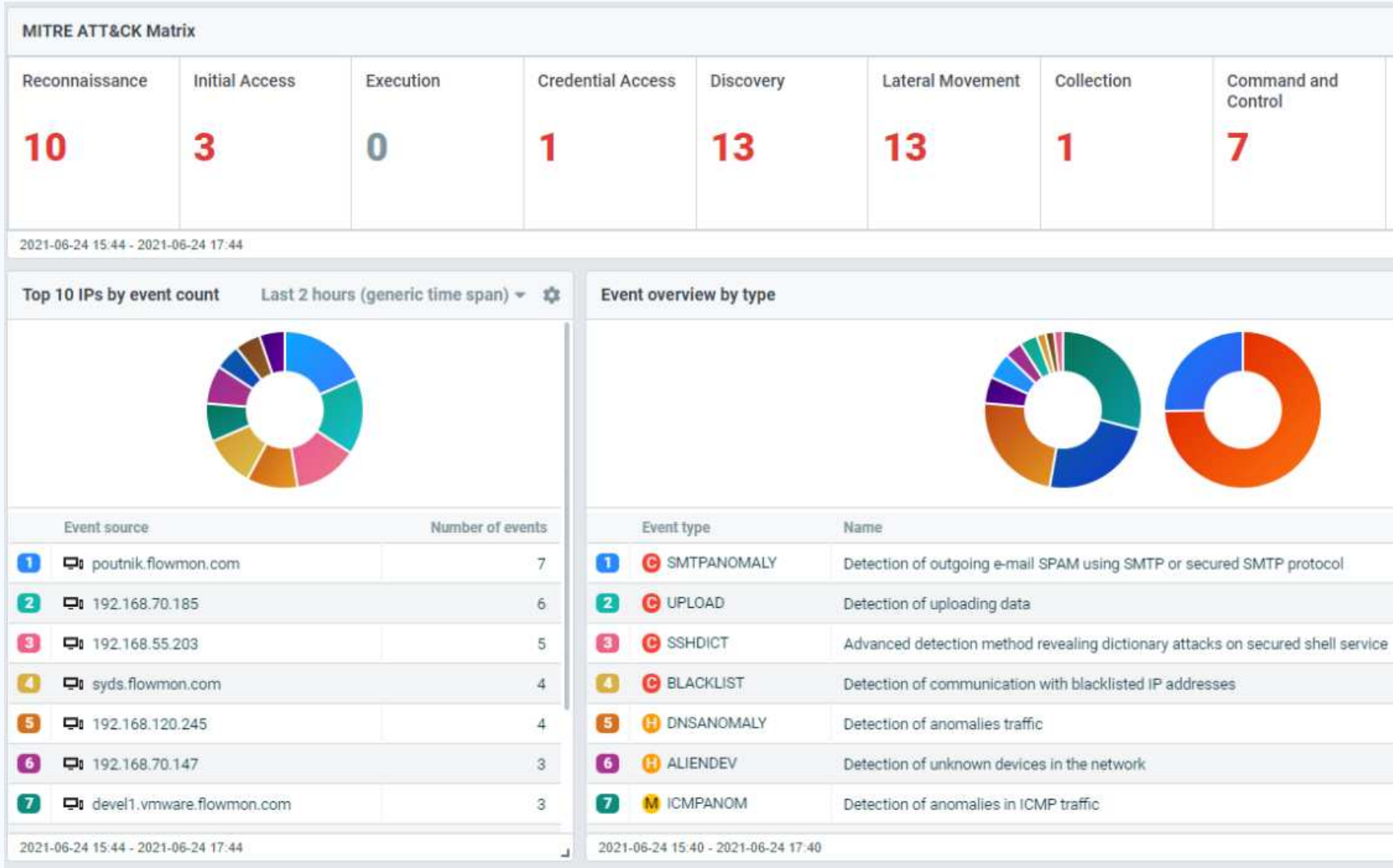


(ADS)

Automātiskā noteikšana un reaģēšana (NDR)

Pateicoties vairāk nekā 40 uz AI balstītām metodēm un 200+ algoritmiem, draudi tiek atklāti laicīgi un pilnībā automātiski. Atklājiet nezināmus draudus, ļaunprātīgu programmatūru, izspiedējvīrusa programmatūru, Windows DNS SIGRed izmantošanu, Trojas zirgu uzbrukumus vai šifrētā trafikā paslēptus draudus.

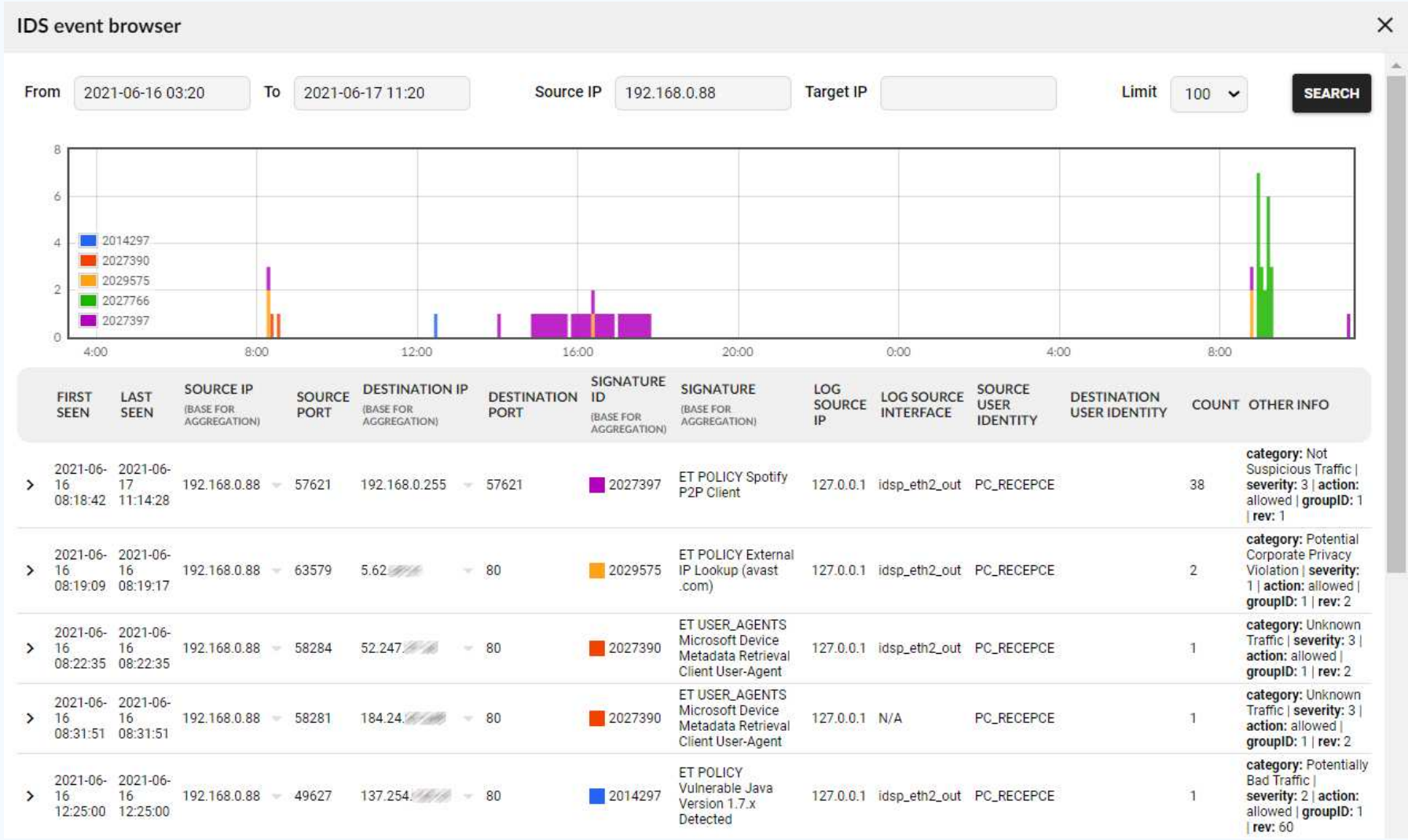
ADS var integrēt ar tīkla piekļuves kontroles sistēmām, ugunsmūri un citiem rīkiem tūlītējai reaģēšanai uz incidentiem (API). + SIEM



(ADS)

Probe + Suricata

Pateicoties Probe (Sensora) iebūvēto Suricata funkcionalitāti – ir iespēja papildināt uzbrukuma vectoru atpazīšanu – apvienojot gan ‘Signature-less un Signature-based’ uzbrukumu identificēšanas pieejas.



Suricata is a high performance, open source network analysis and threat detection software used by most private and public organizations, and embedded by major vendors to protect their assets.

Prioritizācija – False positive mazināšana

Risinājums spēj atšķirt anomālijas no standarta tīkla datu plūsmas. Konstatētie drošības notikumi tiek sarindoti pēc smaguma pakāpes un risinājumā iebūvētās zināšanu bāze uzlabo jūsu situācijas izpratni un paātrina reaģēšanu uz tiem.

OT/ICS/SCADA – tīkla uzraudzība un drošība

OT – Operational Technology Network – ir augsta riska tīkls un no pārvaldības viedokļa bieži vien ieviest kiberdrošības risinājumus (Līdzīgi kā IT tīklā) ir sarežģīti vai pat atsevišķos gadījumos gandrīz neiespējami.

Tāpēc OT tīkla drošības pasākumi parasti aprobežojas ar ugunsmūru izvietošanu OT vides perimetrā, atstājot visu iekšējo trafiku kā aklo zonu.

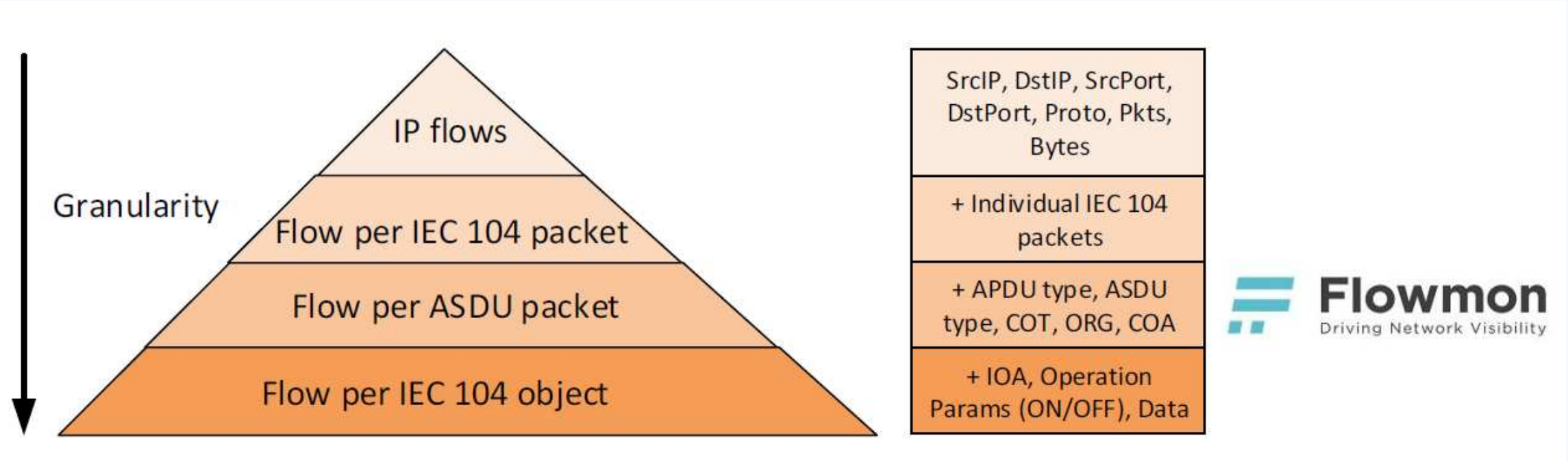
Flowmon piedāvā risinājumu šīs problēmas novēršanai. Jūs vienmēr varat ievietot drošības tehnoloģiju SPAN (spoguļa) portā un izmantot to kā drošības risinājumu, kas nodrošina OT tīkla uzraudzību, problēmu un kiberdraudu noteikšanu.

Tas ir iemesls, kāpēc Flowmon sensori tiek arvien vairāk izmantoti OT vidē, nodrošinot konsolidētu priekšstatu par visu infrastruktūru un ļaujot noteikt anomālijas visā organizācijā.

Galvenā priekšrocība salīdzinājumā ar specializētajiem SCADA drošības rīkiem ir to vispārējā pielietojamība un spēja atpazīt uzbrukumu, pirms tas nonāk OT vidē. Lielākā daļa OT uzbrukumu sākas tradicionālajā IT, un tie atklājas kompromisa rādītājos, kas nosakāmi, izmantojot tīkla uzvedības analīzes pieeju.

OT/ICS/SCADA – tīkla uzraudzība un drošība

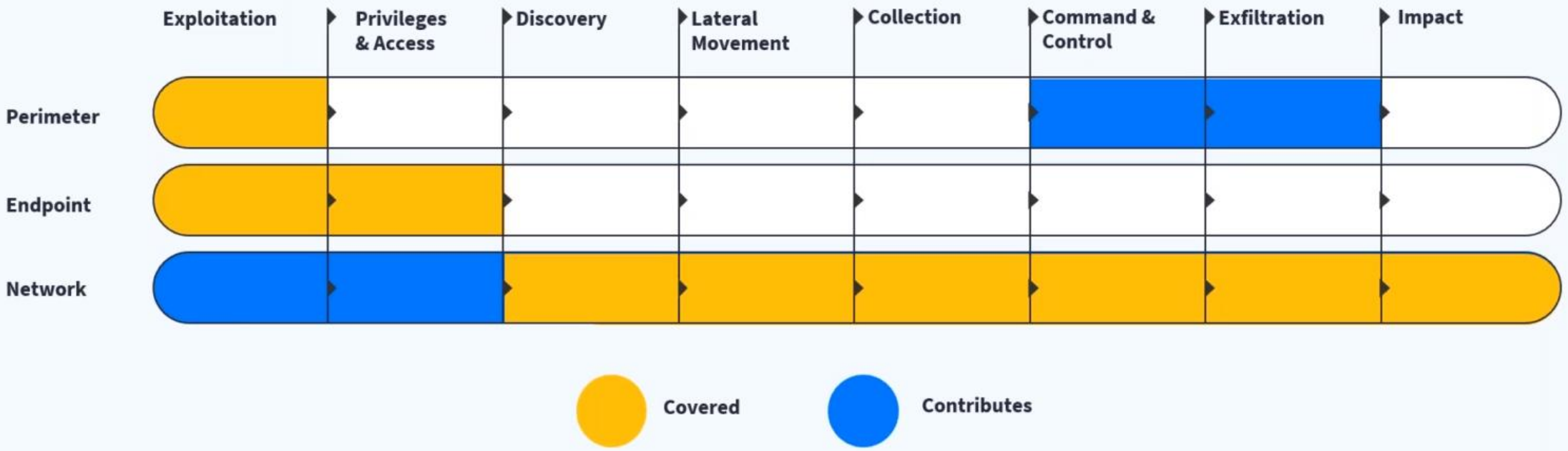
Let us take the IEC 104 protocol used in energy distribution grid control as an example. Extended flow data can provide a valuable insight into application protocols, including OT specifics. Full application level visibility is technically possible due to no encryption.Traditional flow data used to provide an aggregated view of traffic in the OT environment is insufficient to understand traffic patterns, commands or even to recognise malicious activity. Per packet reporting at a header level enables a way to recognise patterns in packet sequences, unfortunately with no way to analyse and interpret the data. Adding application level metadata brings a balance between the level of detail and available information for subsequent analysis. The last option is full packet data; this brings many challenges for performance, data retention, processing and analysis in general. These approaches are presented in figure 1.



https://www.flowmon.com/en/blog/ics-scada-monitoring-and-anomaly-detection

Multi-Layered Security through MITRE ATT&CK Framework

Multiple detection and prevention points are necessary to properly identify ransomware attacks



Flowmon ADS ieguvumi

Automatizācija

Risinājums atklāj draudus un dod ieskatu kiberdraudu analīzē un ieteikumus draudu mazināšanai

Pasīvs / beztrokšņa ieskats

Flowmon sniedz precīzu ieskatu uzbrukuma attēlojumā, izmantojot algoritmus, mašīnmācīšanos, un mākslīgo intelektu.

Zero-day atklāšana

Lietotāji laicīgi uzzina par draudiem, pateicoties uzvedības modeļa analīzei, kas var atklāt anomālijas jau agrīnā stadijā, novēršot iespējamos kiberdraudus.

Īss incidenta reakcijas laiks

Incidenti tiek atklāti gandrīz reāllaikā, nodrošinot kontekstu, tostarp informāciju par incidenta novēršanu.

Flowmon Packet Investigator

Pielietojums

Ar tīkla savienojumu saistītas problēmas

Communication blocked by the firewall, destination unreachable, TCP errors, etc.

Nepareiza darbība vai nepareiza konfigurācija

of critical network services such as ARP, DNS, DHCP

Klienta/servera šifrēšanas nesaderība

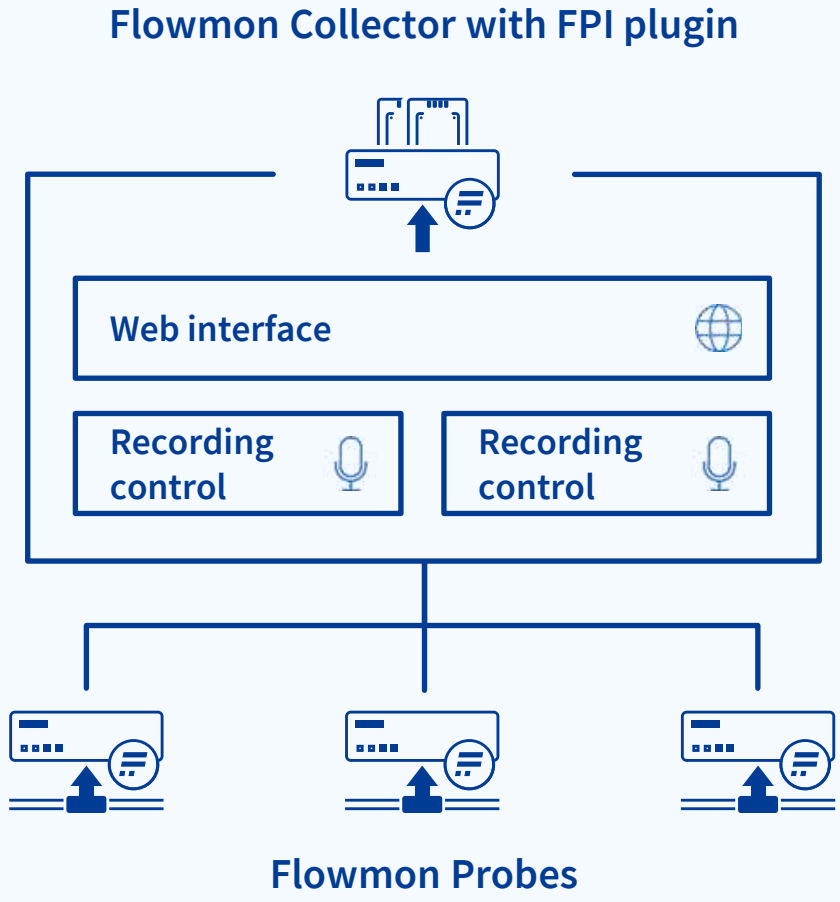
SSL/TLS version, encryption algorithms, certificates, etc.

Lietojumprogrammu protokolu steka problēmas

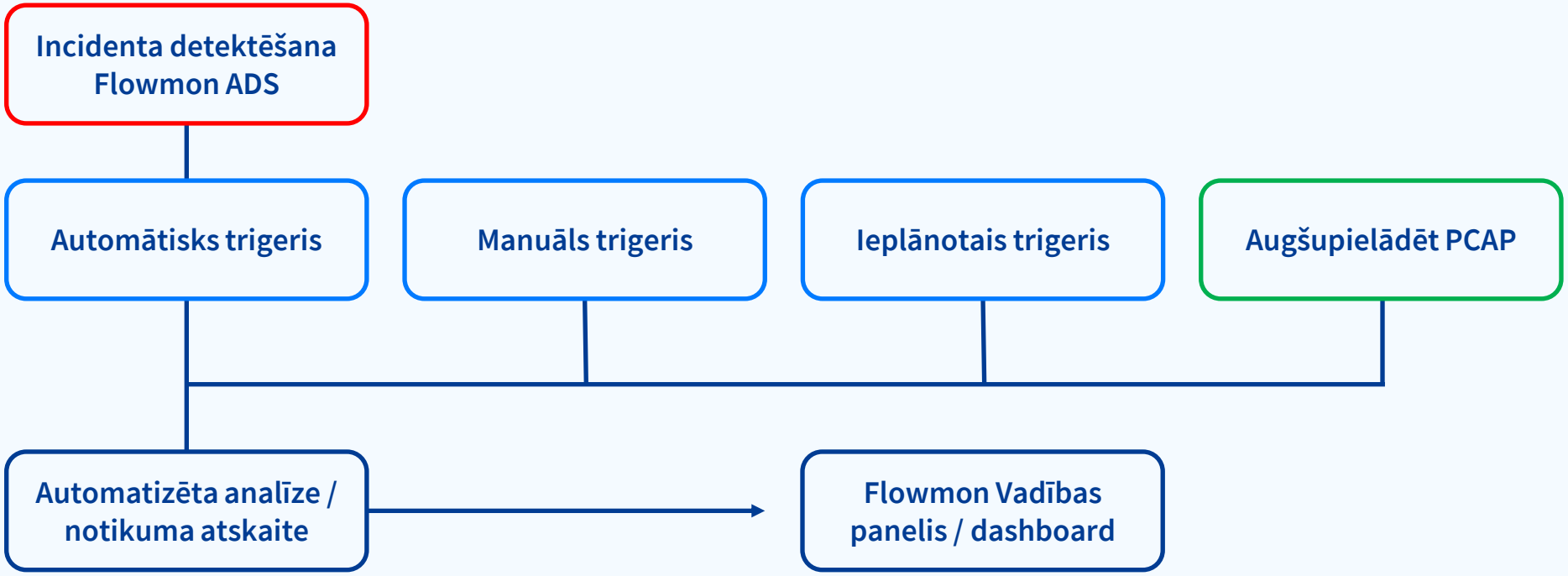
HTTP, SAMBA, FTP, IMAP, POP, etc.

Distributed Deployment

- Flowmon Packet Investigator pilnībā darbojas uz Flowmon sensoriem – probes.
- Centralizēta konfigurēšana un pārvaldība no Flowmon kolektora.
- Mēs varam centralizēti iespējot datu savākšanu pēc parametriem no viena vai vairākiem sensoriem vienlaicīgi.

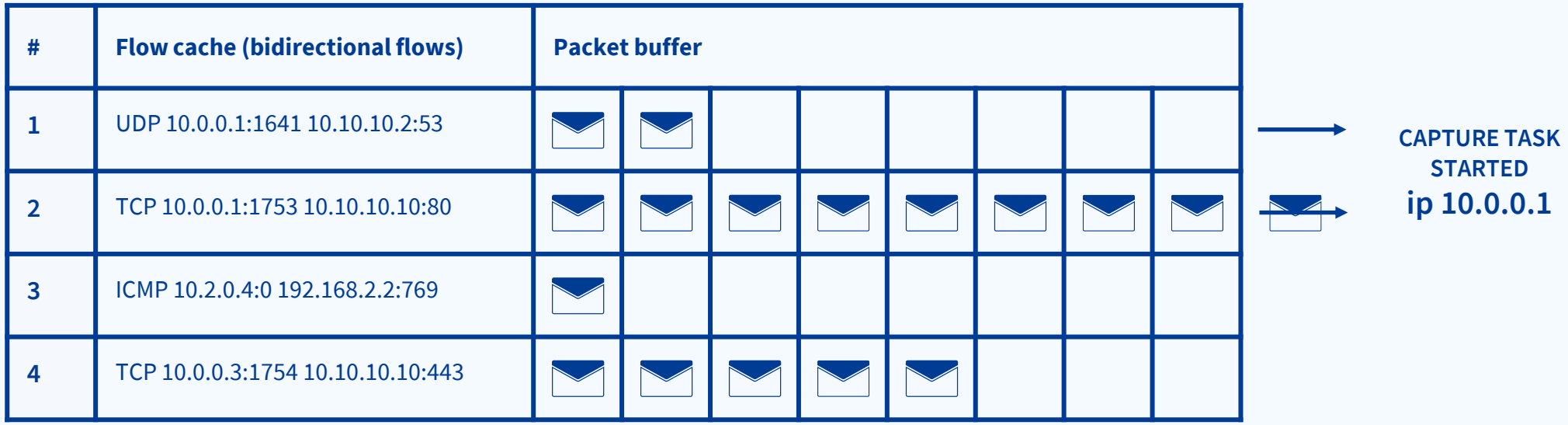


Pakešu ierakstīšanas opcijas



Rolling Capture Buffer

- Recent packets are stored in the memory buffer
  - Buffering the first N (configurable) packets of each flow
  - Rolling buffer with defined capacity (GB) and history (minutes)
- Integration with packet capture
  - Capture task will also extract packets from the buffer
  - Useful for triggered capture based on anomaly detection

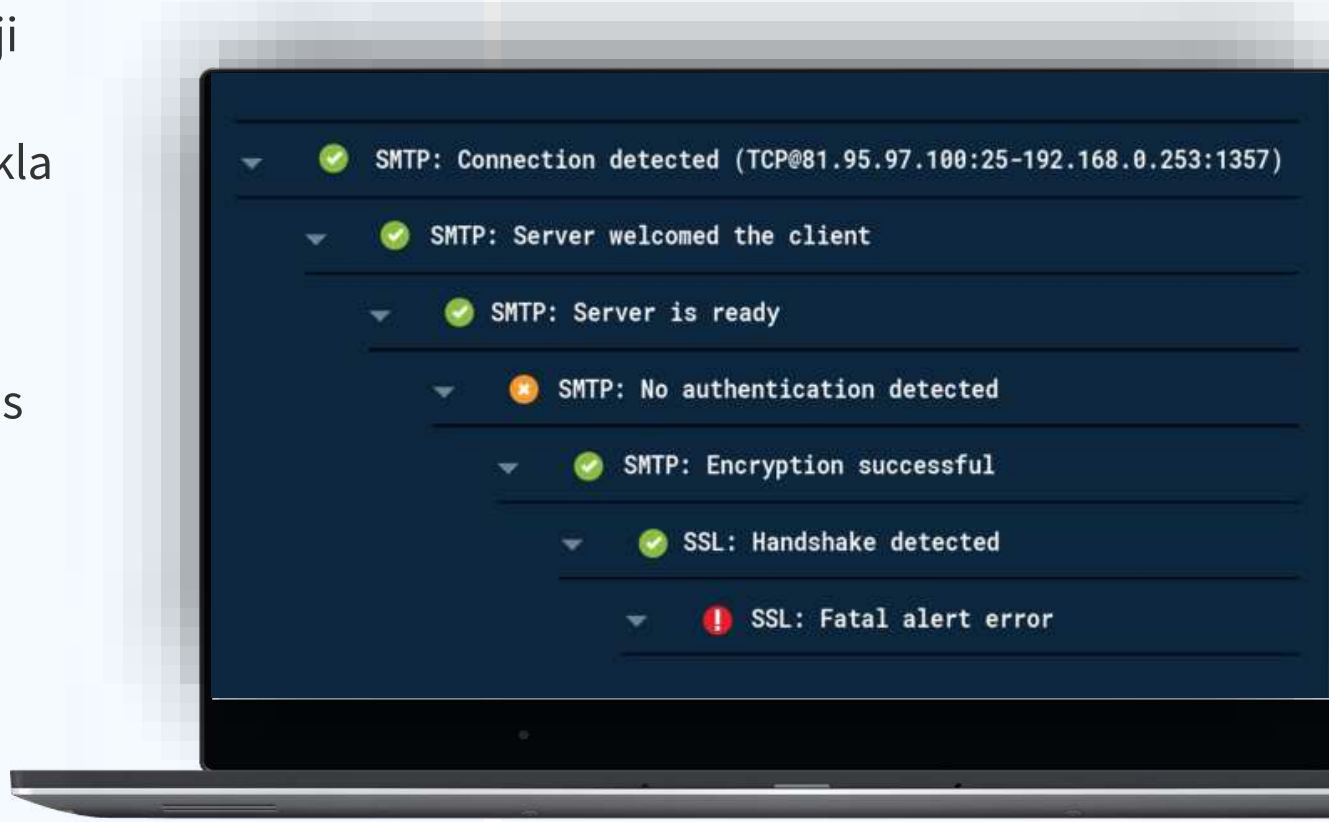


Analīzes modulis – 3 pamata funkcionālās iespējas Intelligent Decision-Tree Analysis

Izmeklēšanas funkcionalitāte - Risinājums sākotnēji automātiski meklē anomālijas pakešu datos (pcap failos) novirzes no biežāk izmantoto tīkla protokolu / servisu normalizētas uzvedības – tai skaitā dažādu tīkla protokolu mijiedarbību, kļūdu kodus un citas neveiksmīgas tīkla darbības.

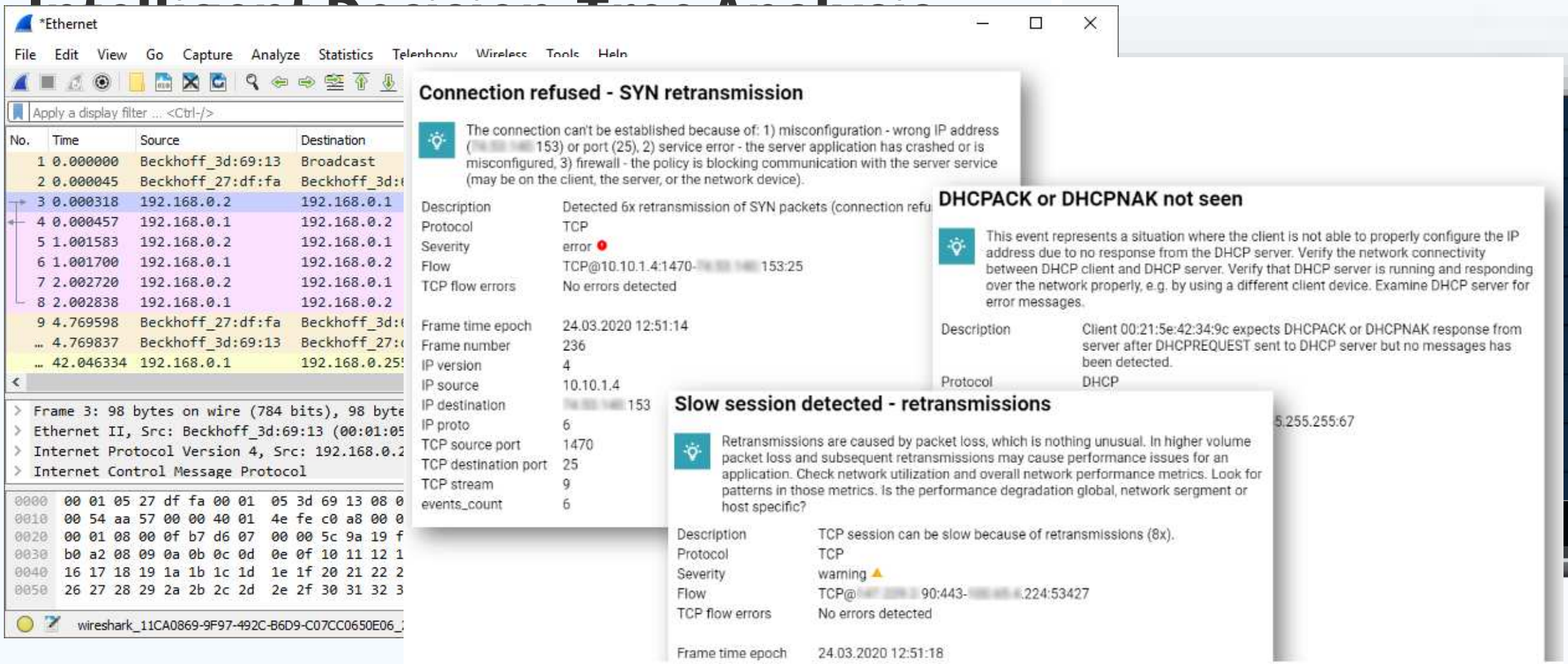
Iebūvētā analīzes ekspertīze – tātad risinājums izmanto iebūvēto kļūdu kodu datu bāzi un pārvērš tos skaidri saprotamā paziņojumā tīkla administratoram vai IT drošībniekam.

Tūlītējas Zināšanas - Rezultāti tiek parādīti informācijas panelī, atbilstoši identificēto problēmu skaitam un kritiskuma pakāpei – kā arī iespējamo ieteikumu problēmas novēršanai, ļaujot tīkla administratoram vai kiberberdrošības specialistam nekavējoties koncentrēties uz attiecīgajām kļūdām un rīkoties.



List of currently supported protocols is the following: ARP, CoAP, DHCP, DNS, FTP, GOOSE, HTTP, ICMP, IEC104, IMAP, IMF, IP, MMS, MQTT, NTP, POP, SIP, SLAAC, SMB, SMTP, SSL and TCP

Analīzes modulis – 3 pamata funkcionālās iespējas



List of currently supported protocols is the following: ARP, CoAP, DHCP, DNS, FTP, GOOSE, HTTP, ICMP, IEC104, IMAP, IMF, IP, MMS, MQTT, NTP, POP, SIP, SLAAC, SMB, SMTP, SSL and TCP

Izmēģinājuma versija

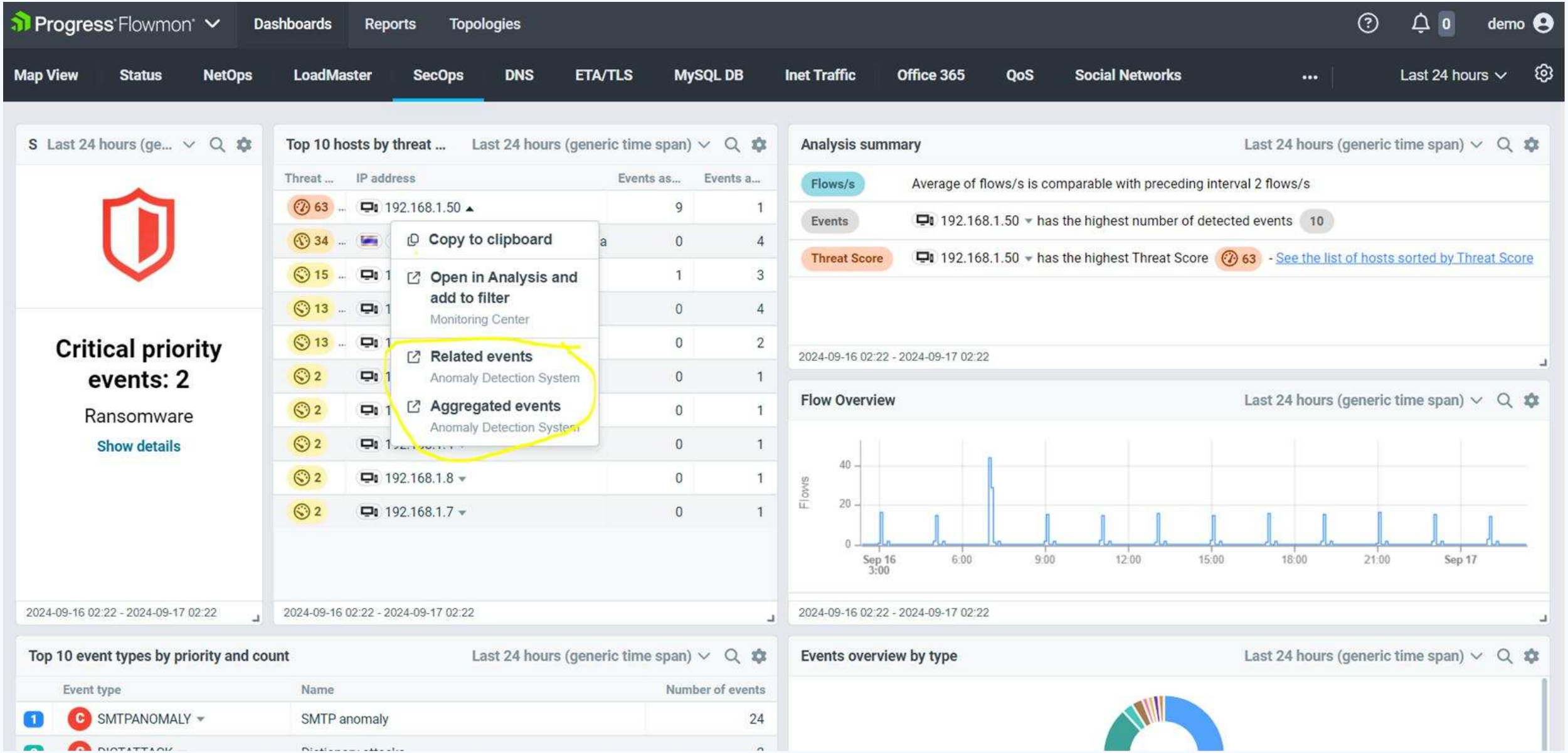
Izmēģinājums -
Jūs iegūsiet pilnu tīkla redzamību ar papildus konfigurētiem moduļiem – kiberdraudu noteikšanā, tīkla darbības analīzē un aplikāciju uzraudzībā.

Izmēģinājuma laikā varēsiet novērtēt savas tīkla infrastruktūras darbību un novērs kļūdas tīkla darbībā, ja tādas tiks identificētas.

Gūsiet ieskatu par tīkla noslodzes rādītājiem, lietotāja parametriem izmantojot publisko internetu un iespēju uzlabot tīkla un aplikāciju darbību.

Iegūsiet papildus aizsardzību no kiberuzbrukumiem un iekšējiem apdraudējumiem ar kiberdraudu anomāliju identificēšanas moduļa palīdzību.

Atbilstība NIS2 Direktīvai, Integrējot Progress Flowmon NDR Risinājumu. 21., 22., 23., 24., 25., 26. pants

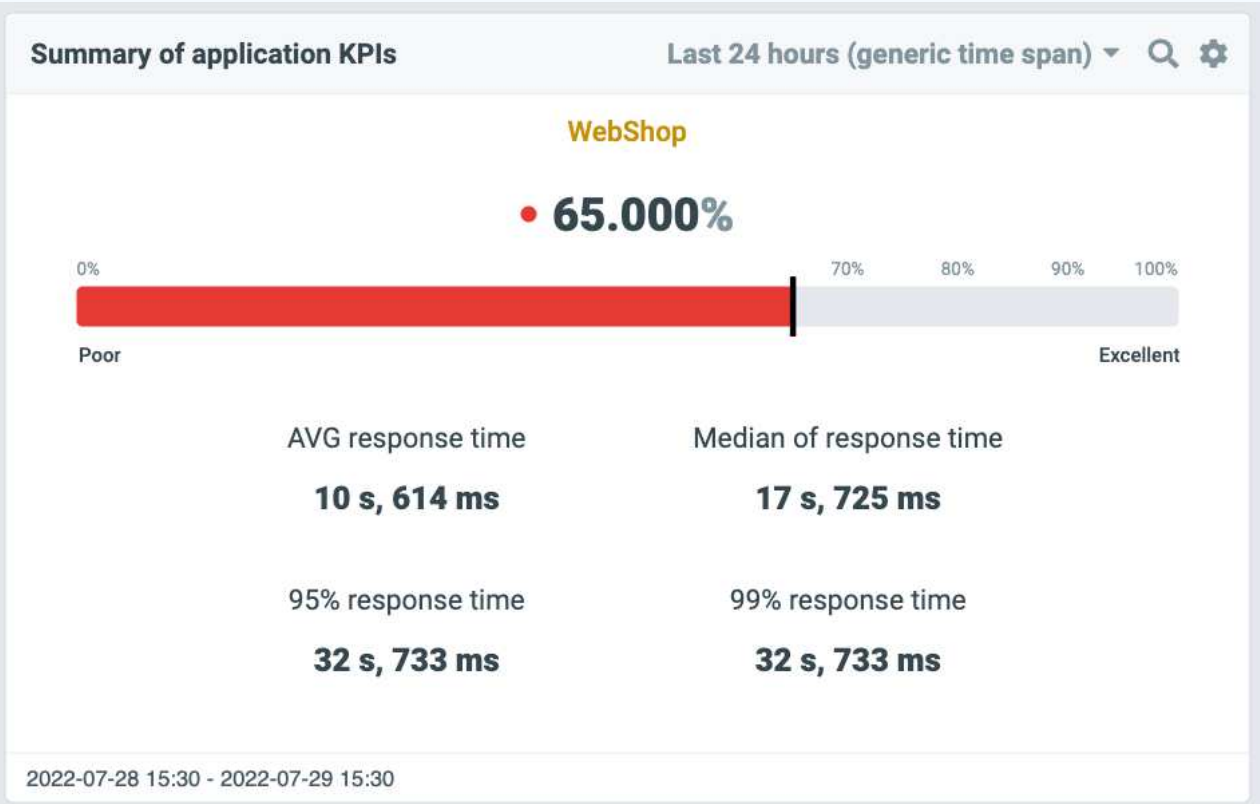


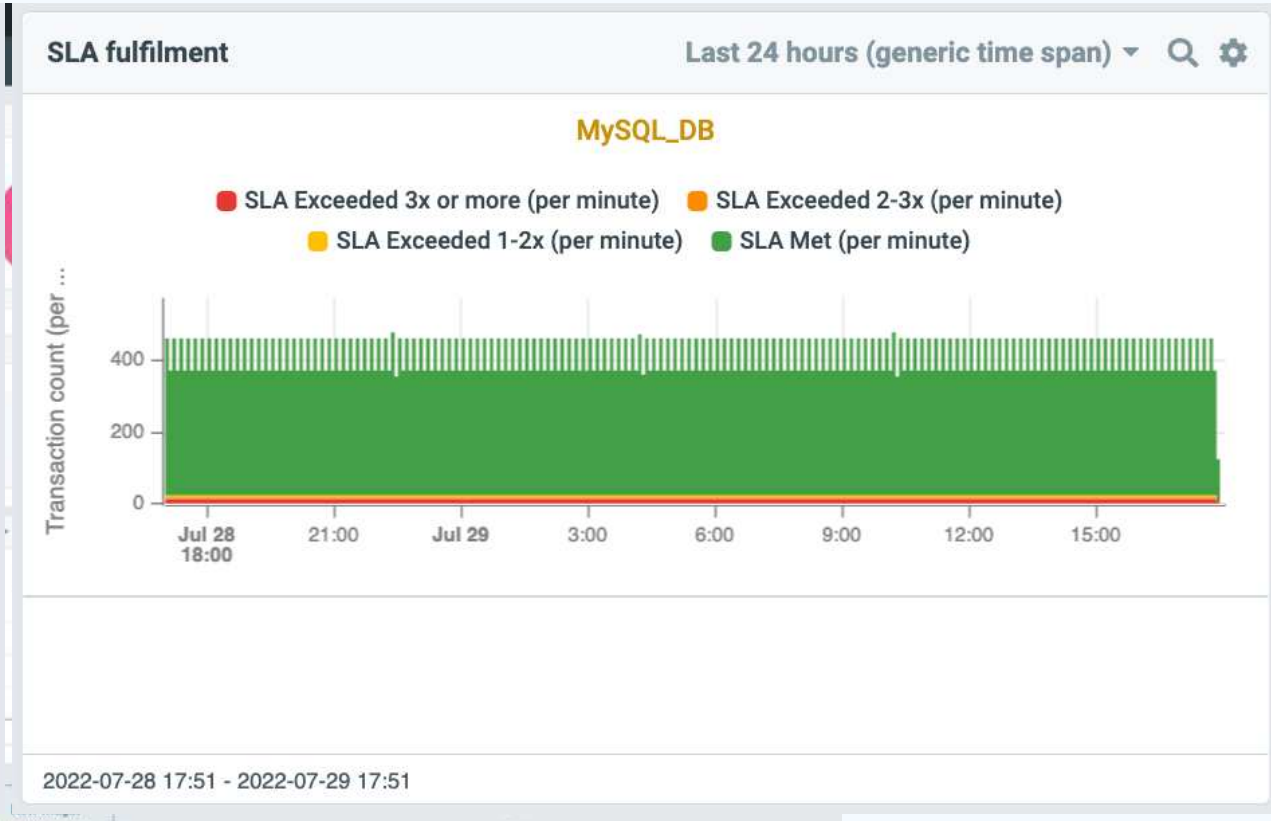
Progress® | Flowmon

Flowmon APM

Aplikāciju uzraudzība (APM)

Flowmon Application Performance Monitoring (APM) ir bezaģentu sistēma, kas mēra lietotāju pieredzi un ziņo par biznesam svarīgu lietojumprogrammu veiktspēju. APM nodrošina datus par lietojumu, jaudu, kļūdu līmeni un SLA, lai paātrinātu problēmu novēršanu un optimizētu lietojumprogrammu pieredzi.





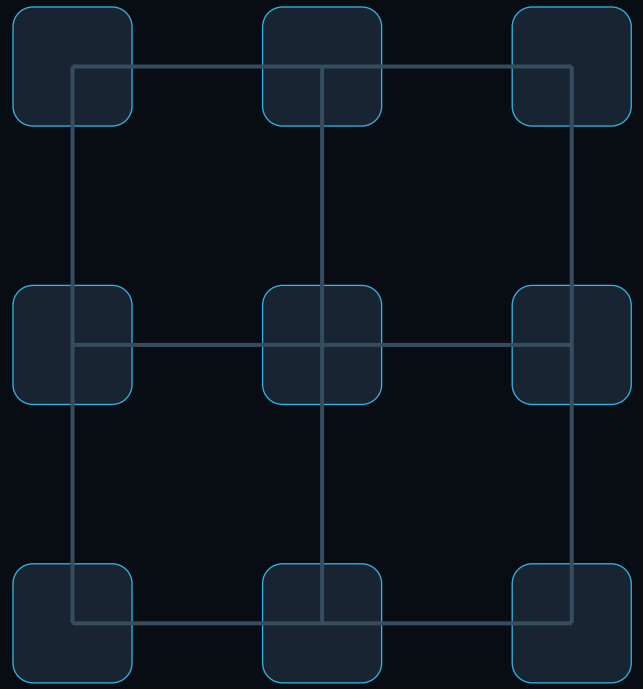
Atbilstība NIS2 Direktīvai, Integrējot Progress Flowmon NDR Risinājumu. 21., 22., 23., 24., 25., 26. pants

NIS2 Direktīvas pants	Prasība	Kā Progress Flowmon NDR nodrošina atbilstību
21. pants: Kiberdrošības riska pārvaldības pasākumi	Ieviest tehniskus un organizatoriskus pasākumus riska pārvaldībai, tostarp:	• Incidentu atklāšana un apstrāde: Reāllaika tīkla trafika uzraudzība anomāliju noteikšanai.
	• Incidentu apstrādi	• Uzlabota draudu atklāšana: Identificē sarežģītus uzbrukumus, izmantojot mašīnmācīšanos un draudu izlūkošanu.
	• Biznesa nepārtrauktību un krīžu vadību	• Audits un reģistrēšana: Nodrošina detalizētus trafika žurnālus audita un atbilstības nolūkiem.
	• Drošības notikumu uzraudzību, auditu un reģistrēšanu	
23. pants: Incidentu ziņošana	Ziņot iestādēm par nozīmīgiem incidentiem 24 stundu laikā un sniegt detalizētu informāciju.	• Agrīna atklāšana un ziņošana: Reāllaika incidentu atklāšana ļauj savlaicīgi ziņot par incidentiem.
		• Visaptveroša ziņošana: Nodrošina detalizētus datus par tīkla anomālijām un incidentu informāciju, kas atvieglo ziņošanas prasību izpildi.
24. pants: Kiberinformācijas apmaiņa	Dalīties ar informāciju par kiberdrošības draudiem un incidentiem ar attiecīgajiem dalībniekiem, lai uzlabotu drošību nozarē.	• Integrācija ar draudu izlūkošanu: Integrējas ar draudu izlūkošanas plūsmām, lai saņemtu jaunāko informāciju par draudiem.
		• Detalizēta trafika analīze: Nodrošina ieskatus, kurus var dalīt ar CSIRT vai citām attiecīgām iestādēm.
20. pants: Piegādes ķēdes drošība	Pārvaldīt drošības riskus piegādes ķēdē, īpaši attiecībā uz trešo pušu pakalpojumiem vai tehnoloģijām.	• Piegādes ķēdes draudu uzraudzība: Uzrauga trešo pušu tīkla trafiku un atklāj aizdomīgas aktivitātes.
		• Draudu virzība: Identificē draudu dzīves ciklu tīklā, lai samazinātu riskus piegādes ķēdē.
25. pants: Kiberdrošības politikas un pārvaldība	Ieviest kiberdrošības pārvaldības pasākumus, tostarp riska novērtējumus un politikas atjauninājumus.	• Politikas ieviešana: Flowmon integrējas ar pārvaldības stratēģijām, nodrošinot nepārtrauktu riska novērtēšanu.
		• Pastāvīga novērtēšana: Uzrauga tīkla uzvedību, lai nodrošinātu drošības politikas nepārtrauktu novērtēšanu.
26. pants: Biznesa nepārtrauktība un krīžu vadība	Nodrošināt būtisku pakalpojumu nepārtrauktību un aizsargāt tīklu krīzes vai incidenta laikā.	• Krīzes vadība: Nodrošina reāllaika draudu atklāšanu un seku mazināšanu, lai atbalstītu biznesa nepārtrauktību.
		• Incidentu izmeklēšana: Piedāvā detalizētu ieskatu, kas atvieglo incidentu analīzi un krīžu vadības uzlabošanu.
22. pants: Tīkla un informācijas sistēmu drošība	Ieviest drošības pasākumus, lai aizsargātu tīkla un informācijas sistēmas no kiberdraudiem.	• Visaptveroša tīkla drošība: Atklāj ļaunprogrammatūru un aizdomīgu tīkla uzvedību, nodrošinot atbilstību drošības prasībām.
		• Nultās dienas (Zero-day) dienas draudu atklāšana: Nodrošina aizsardzību pret uzlabotajiem pastāvīgajiem draudiem (APT) un Zero-day uzbrukumiem.

CASE STUDY | LVM

LVM kiberdrošības incidents:

ko mēs varētu redzēt, pirms kļūst par incidentu?

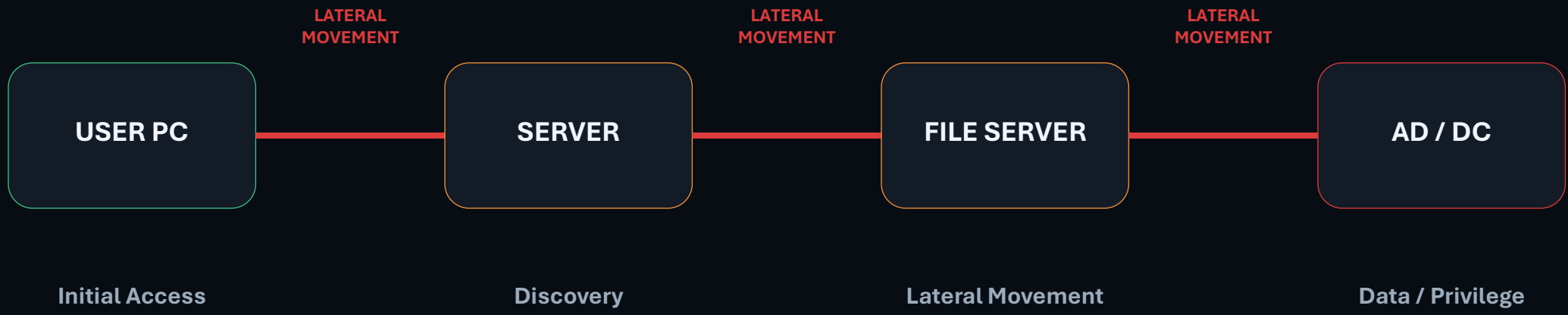


2026. gada 22. jūnijā LVM konstatēja kiberdrošības incidentu IT infrastruktūrā.

GALVENAIS JAUTĀJUMS

Vai mēs redzam pašu uzbrukumu — vai tikai tā sekas?

No viena kompromitēta endpointa līdz infrastruktūrai



Uzbrucējam nav jāpaliek pie pirmā datora. Viņš meklē citus hostus, servisus, kontus un vērtīgus datus.

Ko redz tradicionālā drošības infrastruktūra?

FIREWALL

Internet ↔ Internal

Mazāk redzams
East-West traffic

EDR / AV

Endpoint activity

Ne vienmēr redz
pilnu tīkla kontekstu

SIEM

Logs & events

Atkarīgs no tā,
kas tiek savākts

UZBRUCĒJS JAU IR IEKŠĀ. **Kas redz to, kas notiek starp ierīcēm tīkla iekšienē?**

Ko tīkls pats pasaka par uzbrukumu?

Source | Destination | Port / Protocol | Volume | Frequency | Timing

Ja ierīces uzvedība mainās, Flowmon ADS var to salīdzināt ar tās normālo uzvedību un ģenerēt notikumu.

Kā tas varētu izskatīties LVM scenārijā?

09:14 — Workstation darbojas normāli

09:21 — Neparasta komunikācija ar iekšējiem hostiem

09:26 — Vairāki jauni East-West savienojumi

09:31 — **Reconnaissance / neparasts uzvedības modelis**

09:35 — **Turpmāka kustība iekšējā infrastruktūrā**

FLOW MON ADS

Normal
↓
Deviation
↓
Anomaly
↓
Incident

Ko Flowmon potenciāli dotu LVM scenārijā?

01

IERAUDZĪT

neparastu East-West komunikāciju

02

ATKLĀT

novirzi no ierastās ierīces uzvedības

03

KORELĒT

vairākas aizdomīgas aktivitātes

04

PARĀDĪT

host → host → when → volume

05

KONTEKSTS

incidenta izmeklēšanai

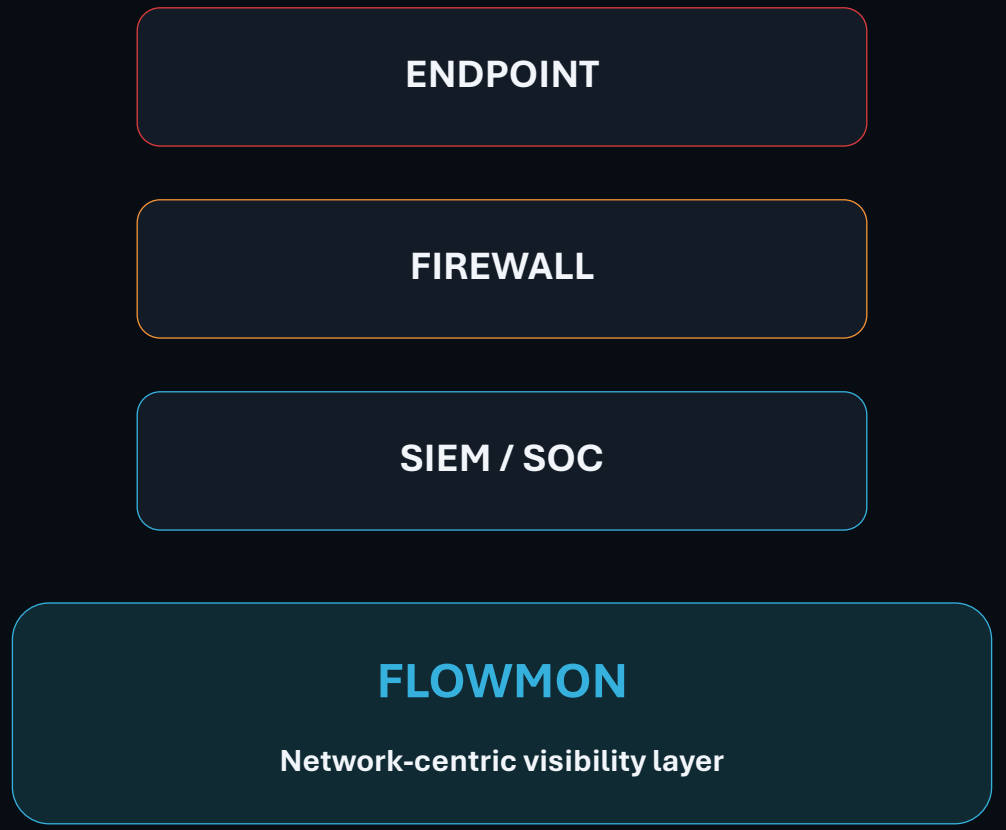
Visibility before impact

Ja ir pieejami nepieciešamie network flow dati, ADS var identificēt uzvedības novirzes un sniegt kontekstu pirms incidenta sekas kļūst acīmredzamas.

So what exactly is Flowmon?

Flowmon

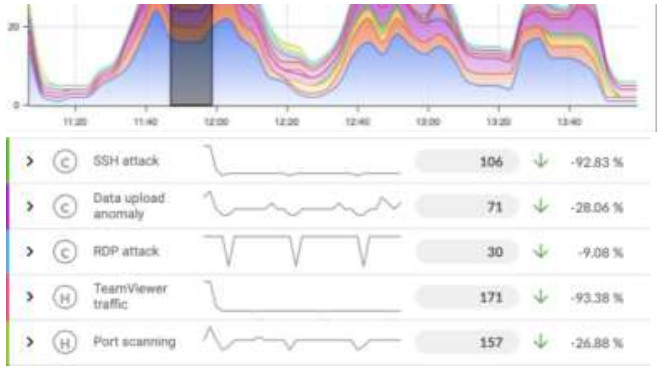
Network Visibility
+
Network Detection & Response



Progress Flowmon

AI-Powered Network Security Analyst Delivered as Software

Powerful detection

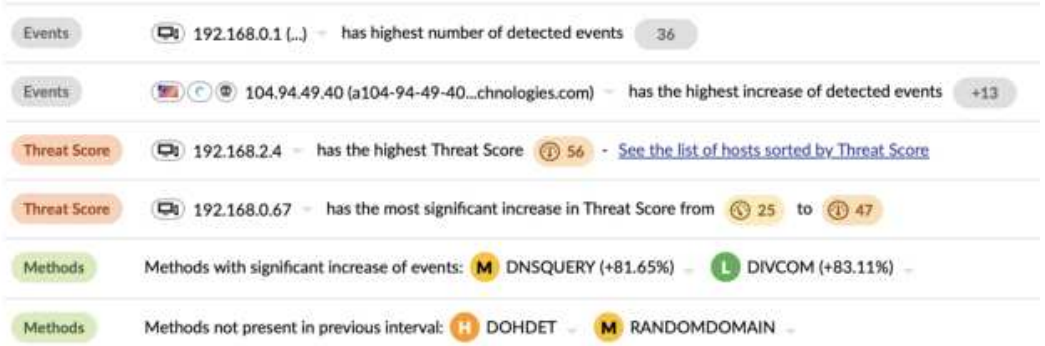


Built in experience

Password rejected

Client was not able to authenticate to FTP server. FTP session cannot be established. Verify login credentials used by FTP client. This event can also indicate an unauthorized attempt to access FTP server.

Smart prioritisation



Automating analytics

Flowmon leguvumi

Automatizēta analītika

Autonomā darbības problēmu pamatcēloņa izmeklēšana, ietaupot stundas vai dienas.

Ekspertīze

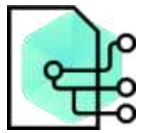
Iebūvētas ekspertu zināšanas par kļūdu kodiem, to apstākļiem un ieteikumiem to novēršanai.

Samazina nepieejamības

Atklājiet anomāliju, izmeklējiet galveno cēloni un automātiski, dažu sekunžu laikā, saņemiet ieteikumu par to, kā rīkoties, lai novērstu incidentu.

Samazina # dažādu rīku izmantošanu

Pieejamība uzraudzība, problēmu novēršana, atbilstība un kiberdrošība — ar Flowmon — centralizēti – izmantojot vienu risinājumu, nepārslēdzoties starp lietotāja interfeisiem.



Padziļināti pierādījumi – tad kad tas ir nepieciešams

Samaziniet troksni, ierakstot tikai to, kas ir būtiski, un saglabājiet to analīzei un auditam pēc incidentu apstrādei


Progress®
Flowmon