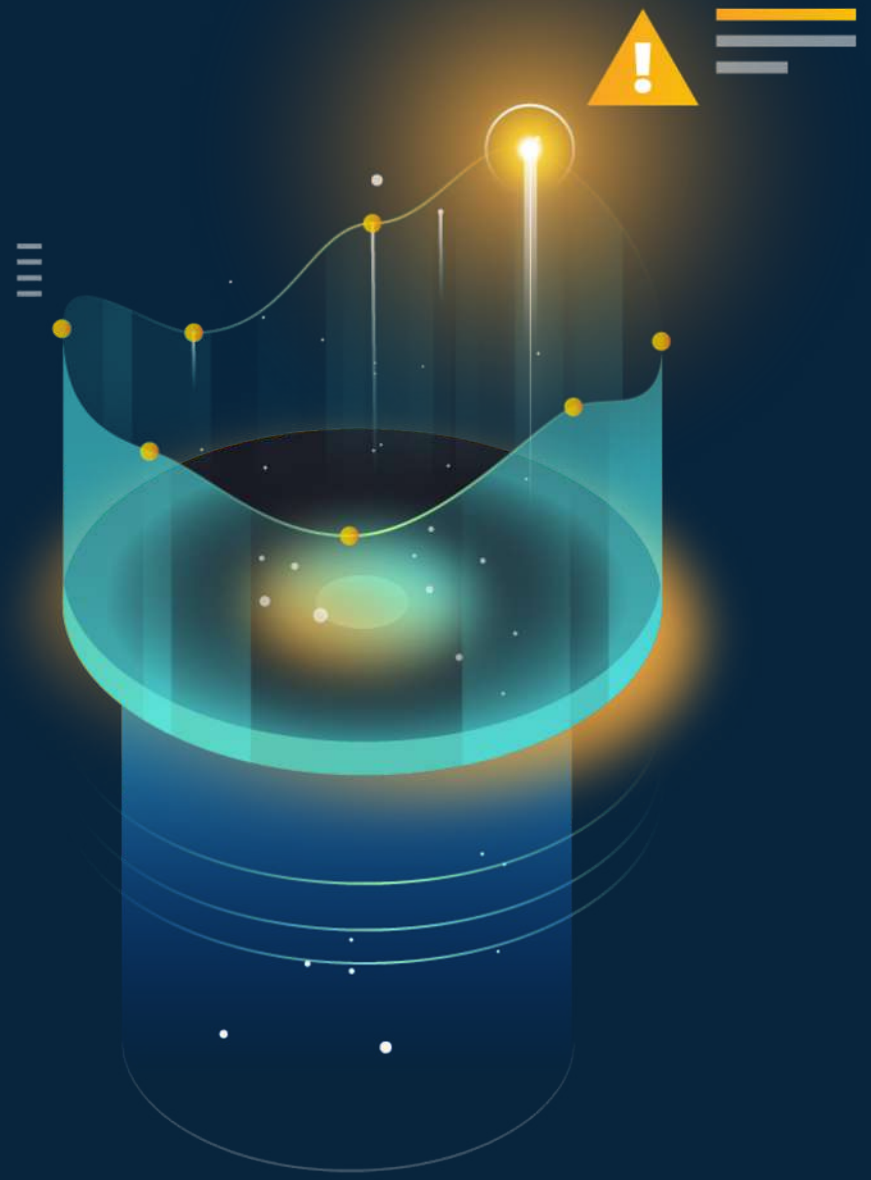
Flowmon Networks

Вирусы атакуют!

Как админу и безопаснику ~~не сойти с ума~~ спасти себя?



Nikolay Brykov | Presales Engineer

Глобальная политика

Нет командировкам

Нет личным встречам

Рост количества домашних офисов

Влияние

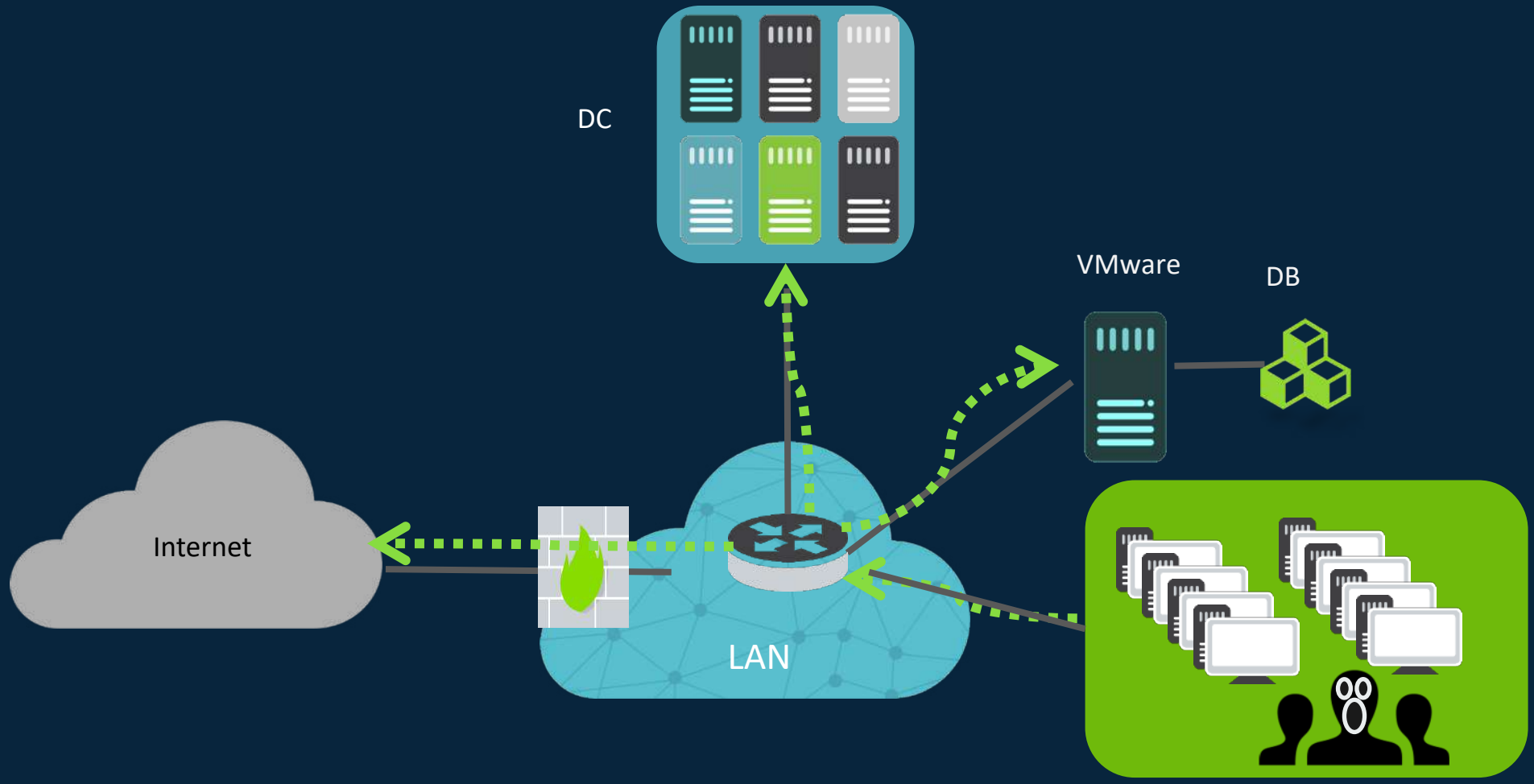
Больше аудио/видео коммуникаций

Бóльшая загрузка Internet uplink (in/out)

Больше VPN трафика

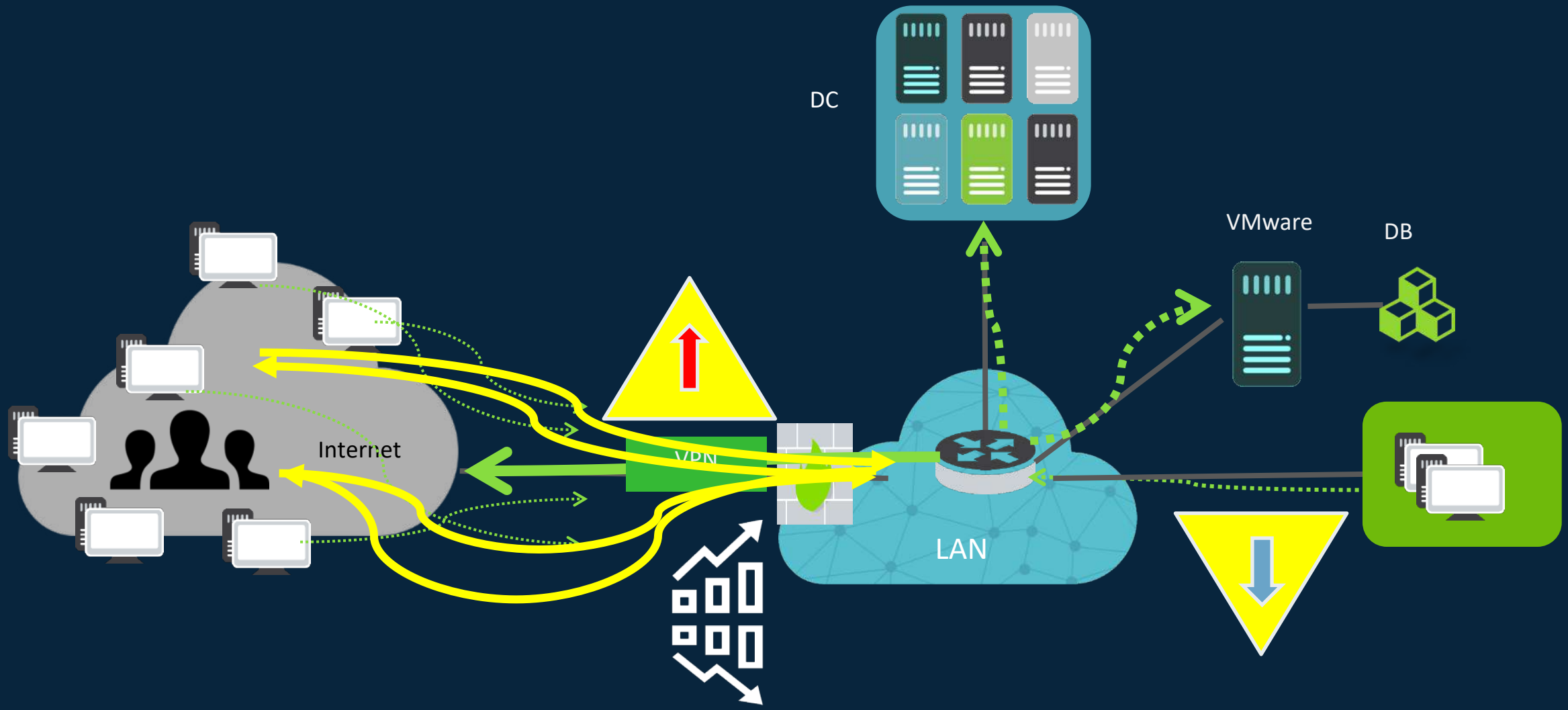
Стандартная рабочая модель

Подключение к локальным ресурсам внутри LAN или по выделенному каналу в DC



Home office

Подключение к локальным ресурсам через VPN
Internet коммуникация через HQ



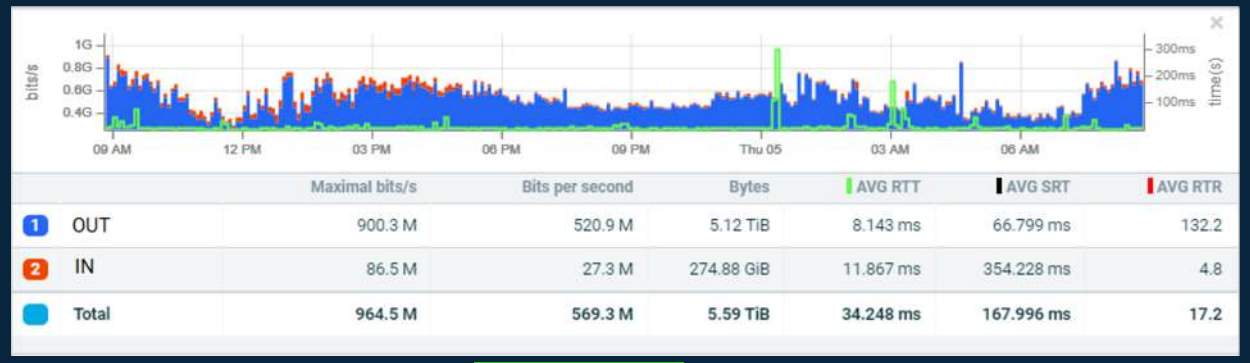
А ваша сеть готова к этому?
Как отреагировать на увеличение пропускной способности?

Please wait…

- Использовать облачные сервисы?
- Расширить канал связи?
- А что если проверить производительность сети и пользователей?

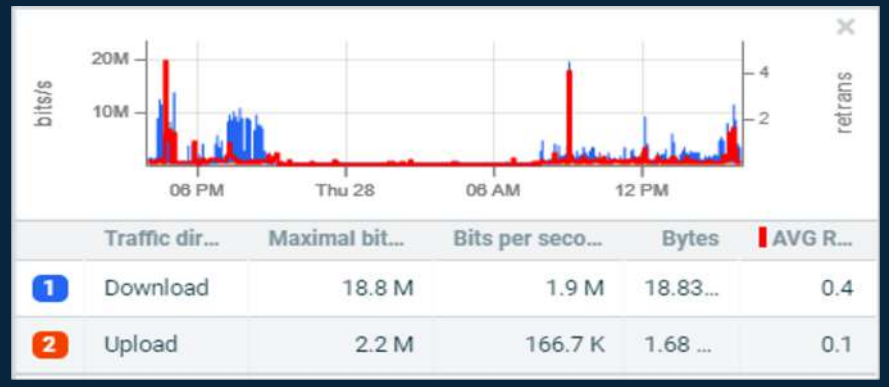
Сетевой мониторинг с Flowmon

Утилизация Uplink
VPN in/out статистика
Метрики производительности сети – network delay (RTT), retransmissions, jitter
Аудио/Видео статистика
Деятельность malware



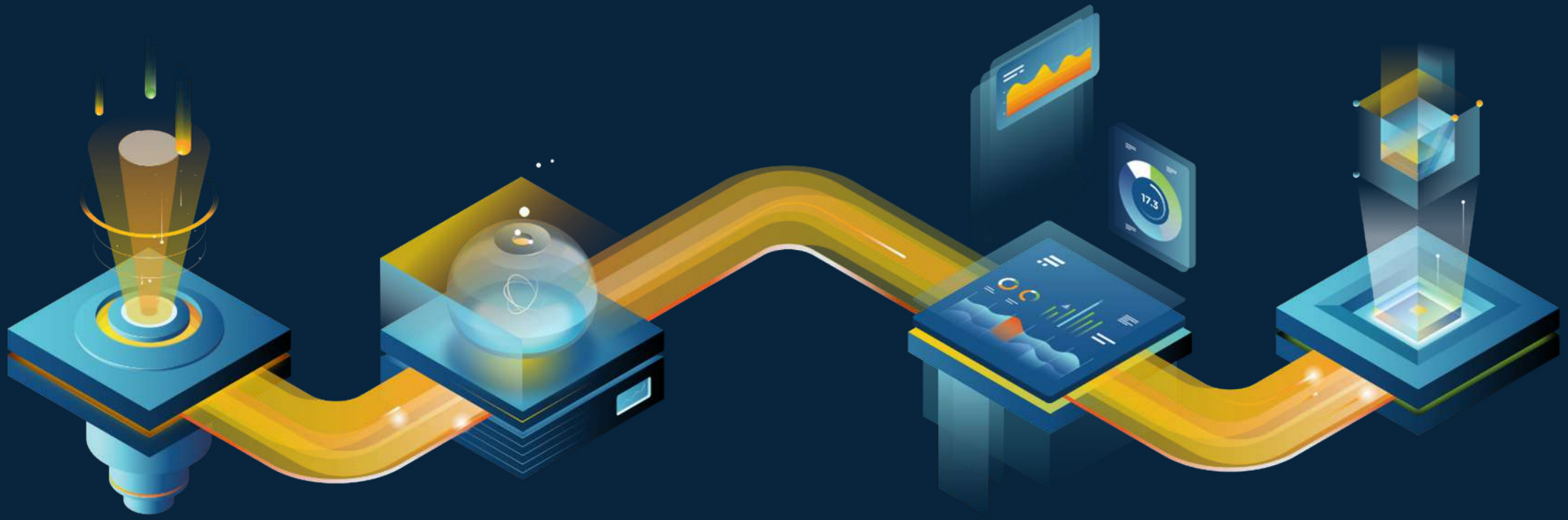
		Maximal bits/s	Bits per second	Bytes	AVG RTT	AVG SRT	AVG RTR
1	OUT	900.3 M	520.9 M	5.12 TiB	8.143 ms	66.799 ms	132.2
2	IN	86.5 M	27.3 M	274.88 GiB	11.867 ms	354.228 ms	4.8
	Total	**964.5 M**	**569.3 M**	**5.59 TiB**	**34.248 ms**	**167.996 ms**	**17.2**

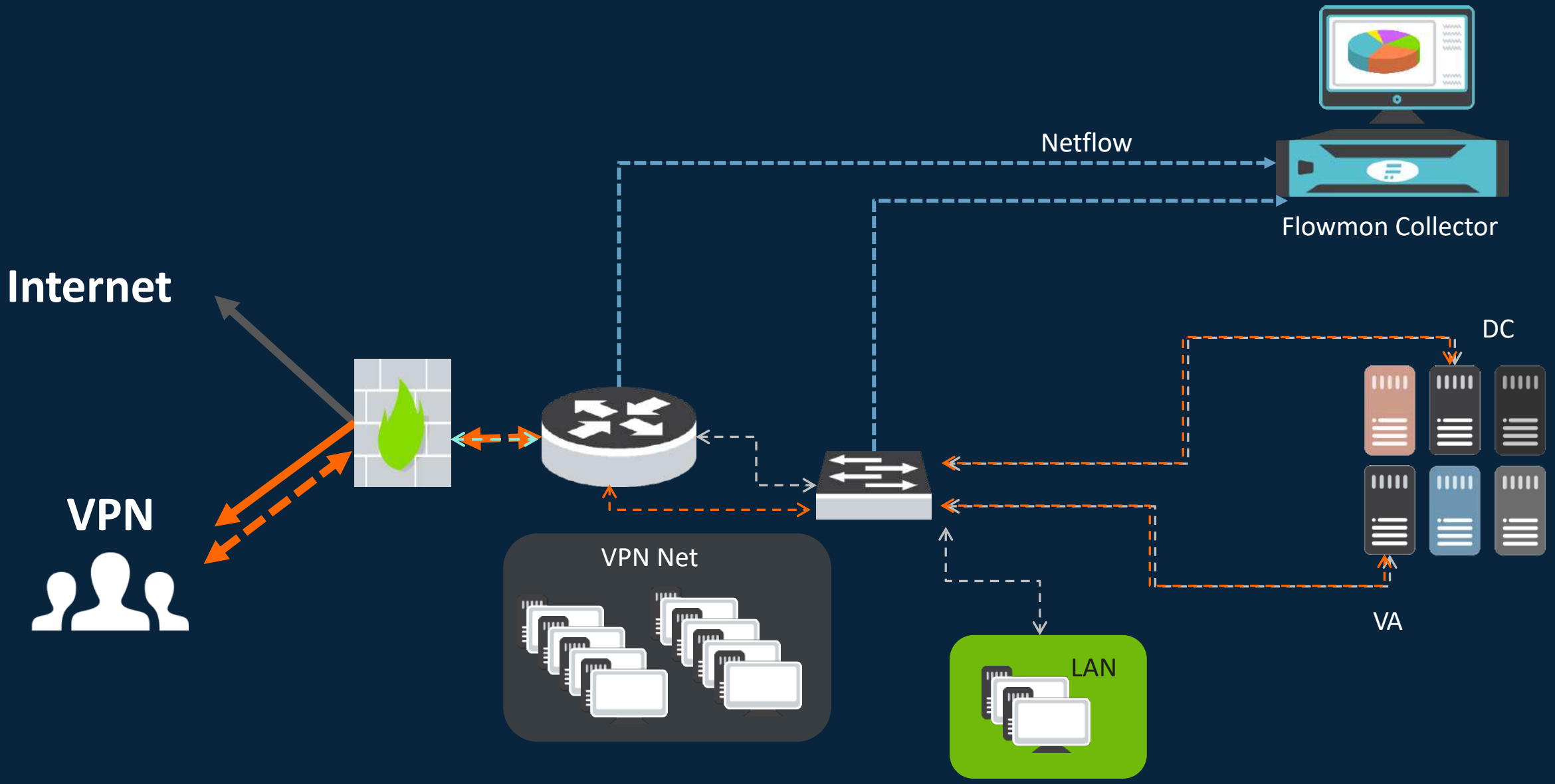
VPN



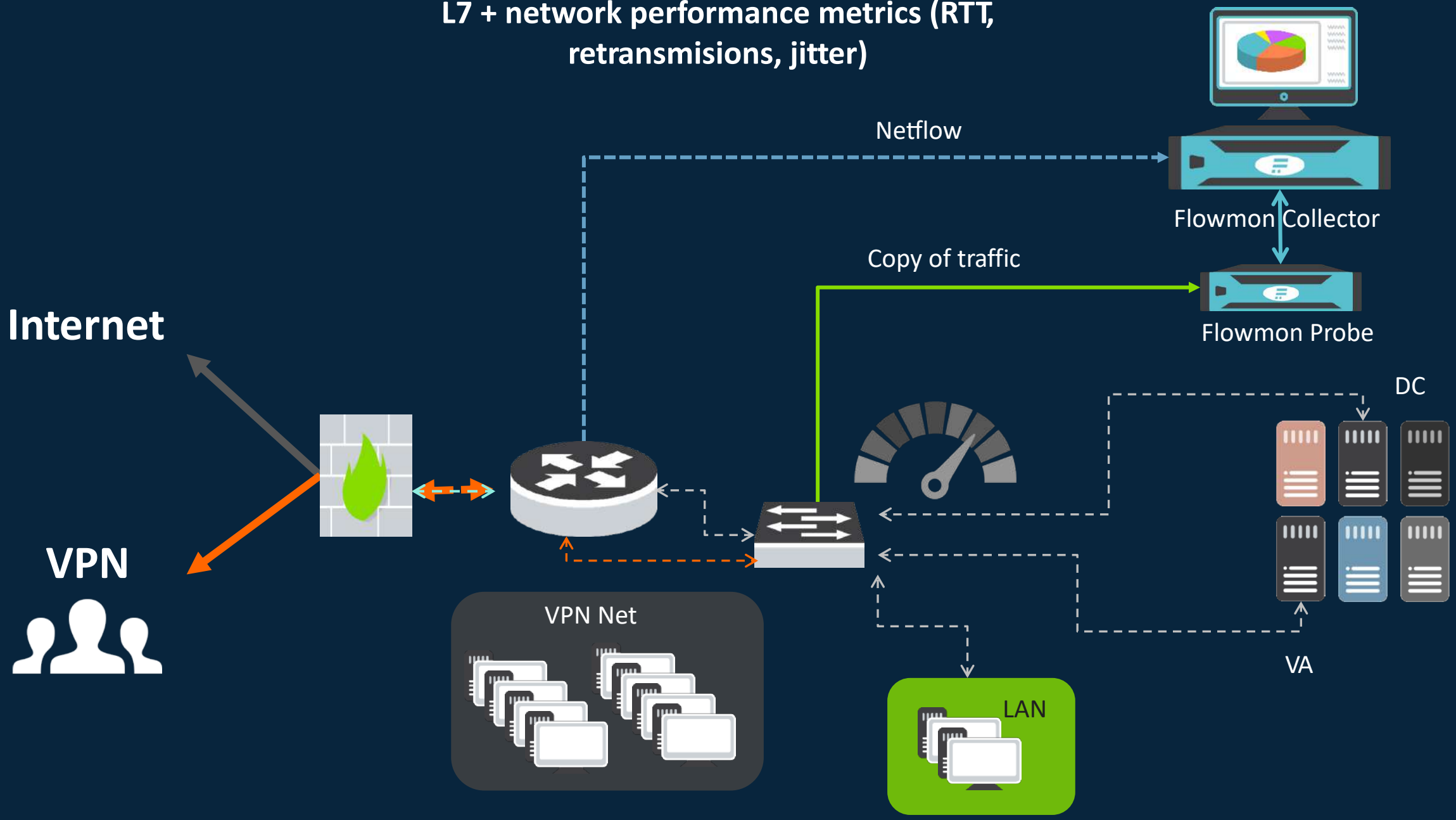
	Traffic dir...	Maximal bit...	Bits per seco...	Bytes	AVG R...
1	Download	18.8 M	1.9 M	18.83...	0.4
2	Upload	2.2 M	166.7 K	1.68 ...	0.1

Внедрение




Netflow
Flowmon Collector
Internet
DC
VPN
VPN Net
VA
LAN

L7 + network performance metrics (RTT, retransmisions, jitter)



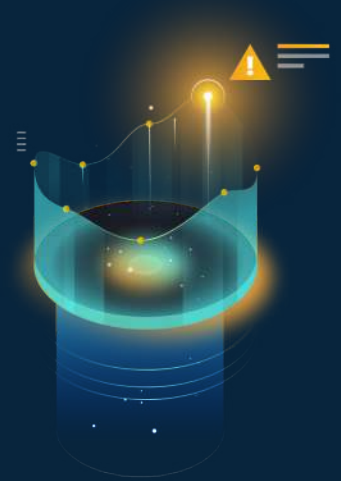
Общие цели. Одно решение.
Самое быстрое в отрасли Time-To-Value.

Мониторинг и Диагностика производительности сети для NetOps

- Мониторинг взаимодействия с конечными пользователями
- Устранение неполадок
- Прогнозирование и планирование
- Cloud/SaaS Performance

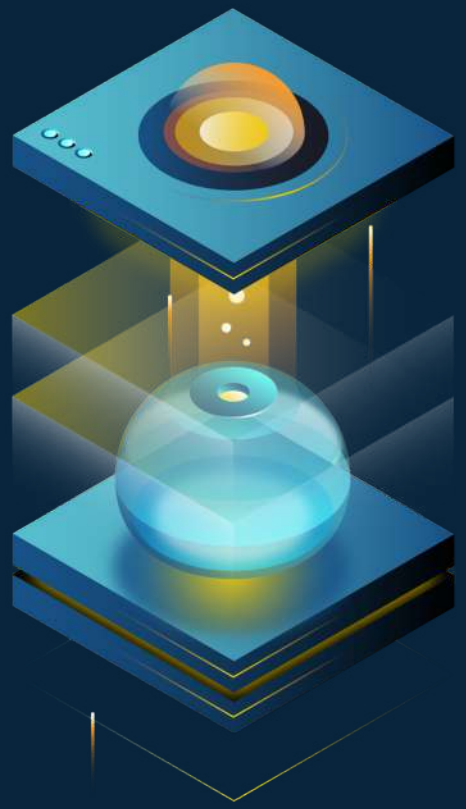
Избавление от границ между NetOps and SecOps

- Дизайн и проектирование инфраструктуры
- Мониторинг и расследование проишествий
- Реакция на инцидент
- Применение и проверка политик



Анализ сетевого трафика для SecOps

- Обнаружение неизвестных угроз
- Анализ шифрованного трафика
- Обнаружение внутренних угроз
- Network Behavior Analysis (NBA)



Live Demo Use Cases

- Flowmon Dashboard (Home Office & Remote Users)
- Утилизация канала
- Какой тип связи больше всего утилизирует VPN трафик
- Измерения производительности сети
- VPN угрозы и атаки (PROXY, RDP, C2)

Чеклист для компаний с удаленными сотрудниками

Organization

- Создание **инструкции** для удаленных сотрудников
- Разработка и проведение **тренинга по работе из дома**
- Выбор **видеоконференции** и **backup платформы**
- Создание **коммуникационного плана** для привлечения пользователей к ежедневным активностям

Security

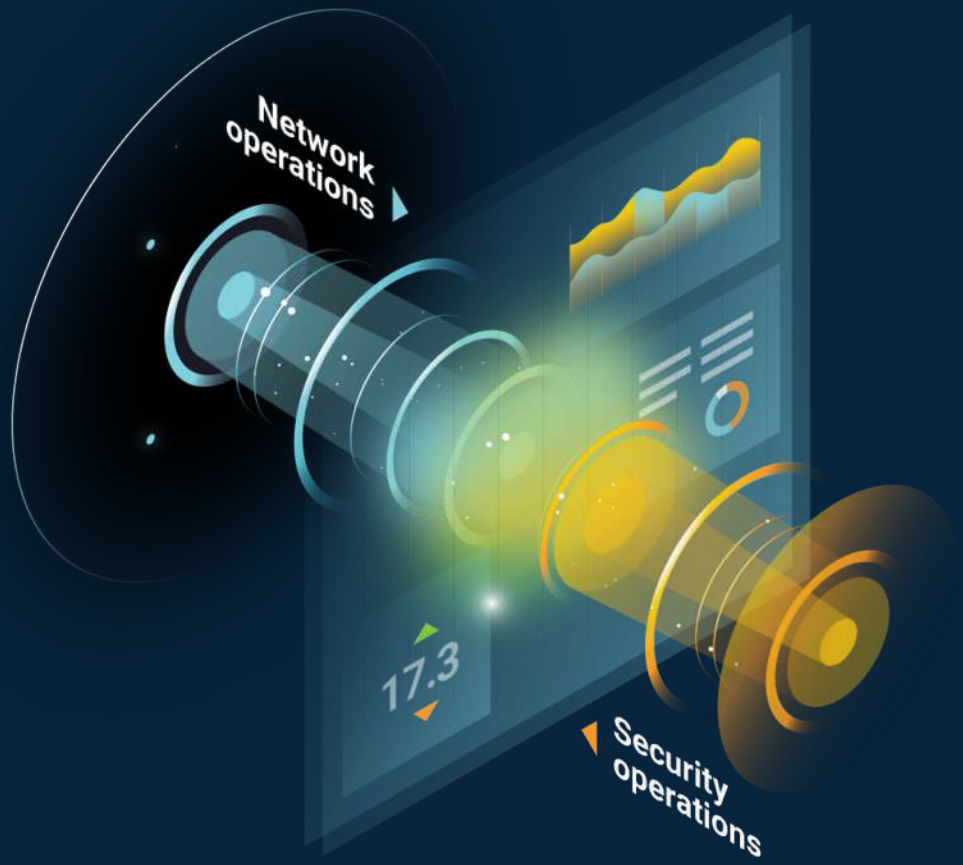
- Внедрение **Zero Trust architecture** в вашей сети
- Убедиться, что на **всех устройствах** установлена **последняя версия ОС**, все **обновления** безопасности и приложений.
- **Убедиться,** что все удаленные работники имеют **VPN доступ**
- **Проинструктировать** персонал **о** возникающих **угрозах безопасности** (фишинг, кража VPN creditials)

Infrastructure

- Убедиться, **что вы имеете достаточную ширину канала** входящего в офис
- Убедиться, что **сотрудники имеют доступ** к вашим **облачным приложениям** и сервисам **напрямую**
- Быть уверенным, что **backup-ы всех сервисов есть** и они **рабочие**, чтобы сотрудники могли продолжить работу в случае отказа основных сервисов
- **Контролировать** и **мониторить весь сетевой трафик** для избежания любых операционных проблем или проблем безопасности

Flowmon
Networks

Thank you!



Nikolay Brykov | Presales Engineer
nikolay.brykov@flowmon.com