NETWELL

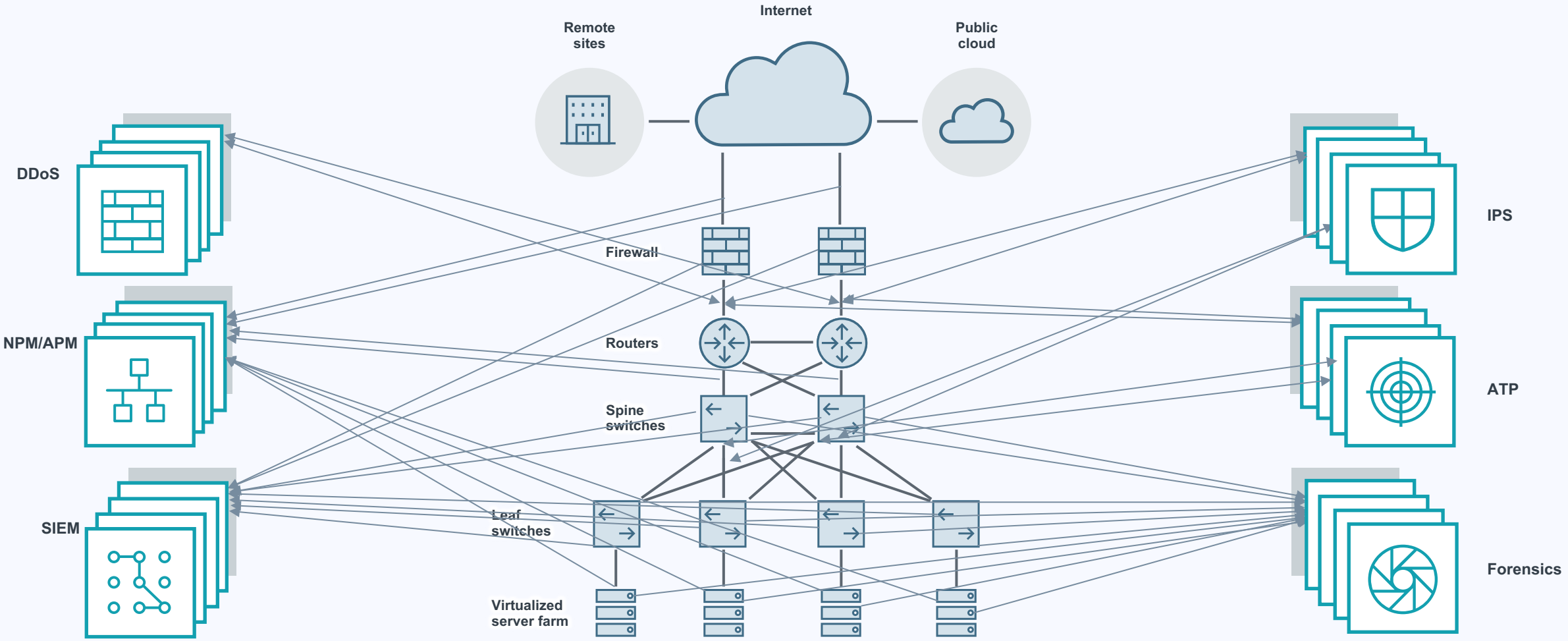
Пакетные брокеры

Видеть больше, защищать надежнее

Александр Грачев
BDM Netwell

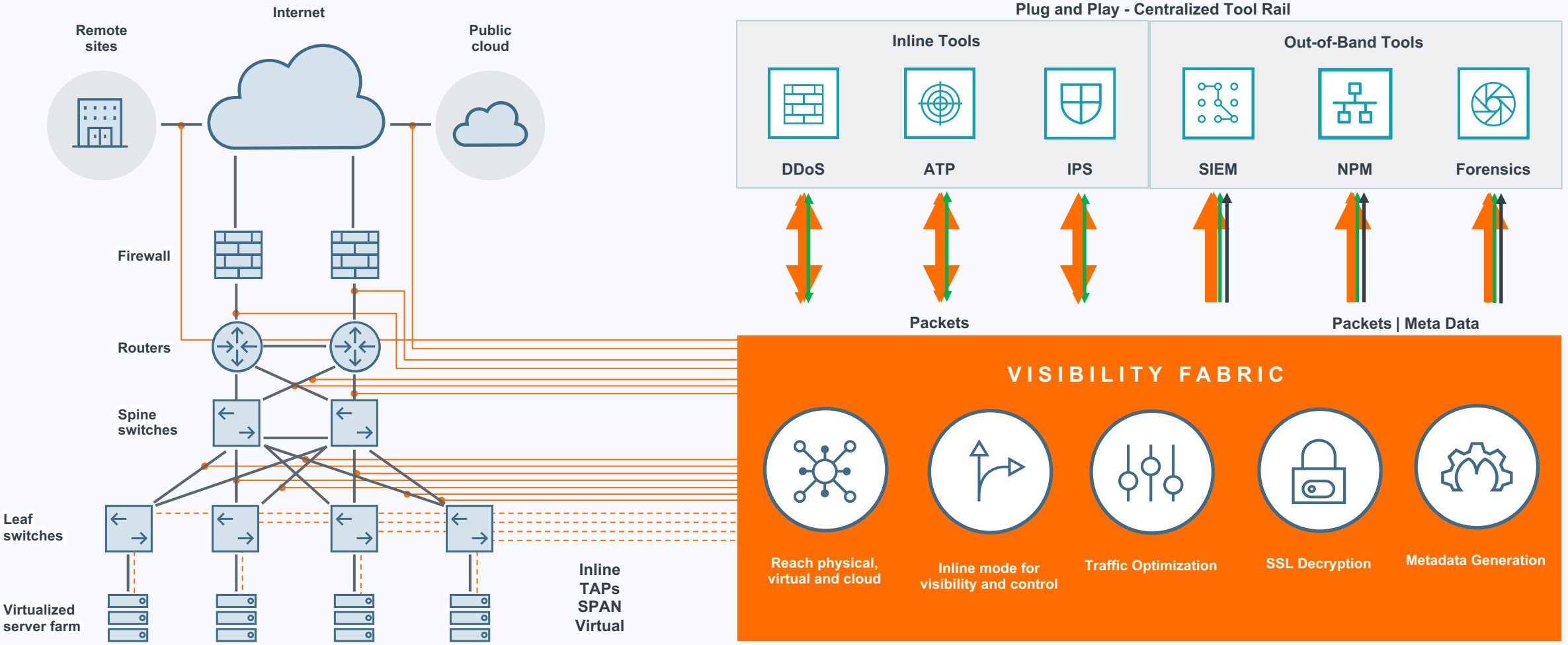
Сеть без пакетных брокеров

Сложный дизайн и проблемы с масштабированием	Получатели перегружены лишним трафиком	Слепые зоны и конкуренция за доступ к копии трафика	Проблемы с шифрованным трафиком и дублированными пакетами	Повышенная нагрузка на сеть и сетевое оборудование



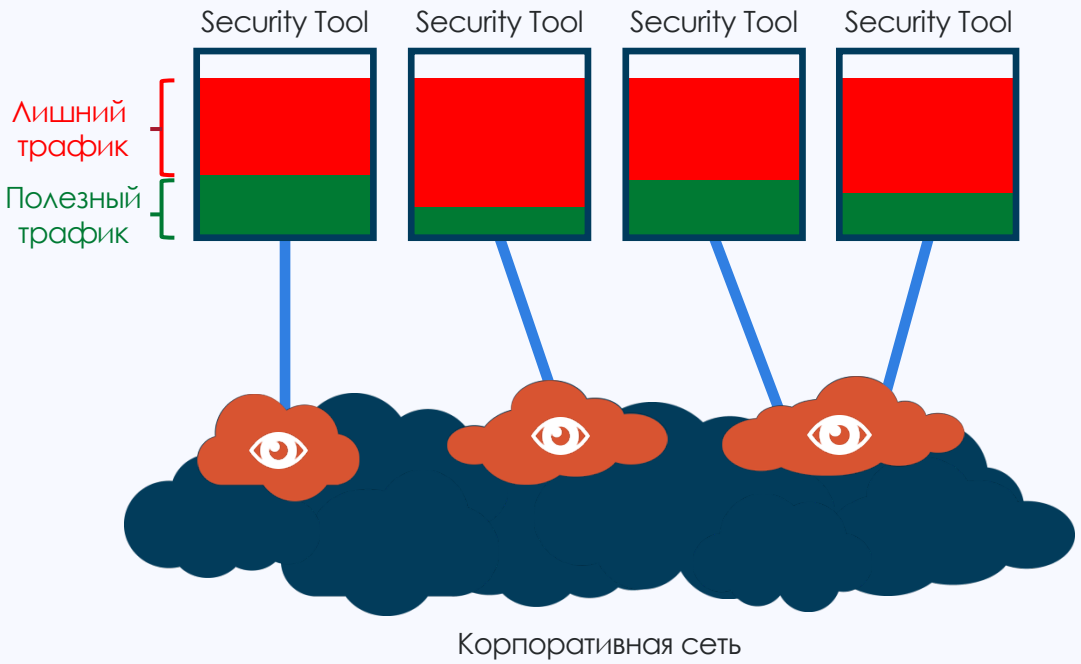
Сеть с пакетным брокером

Простая, легко масштабируемая архитектура	Повышение эффективности получателей трафика	Нет слепых зон и конкуренции за трафик	Каждый получает только нужный трафик и в удобном формате	Снижение нагрузки на сеть, минимизация точек отказа



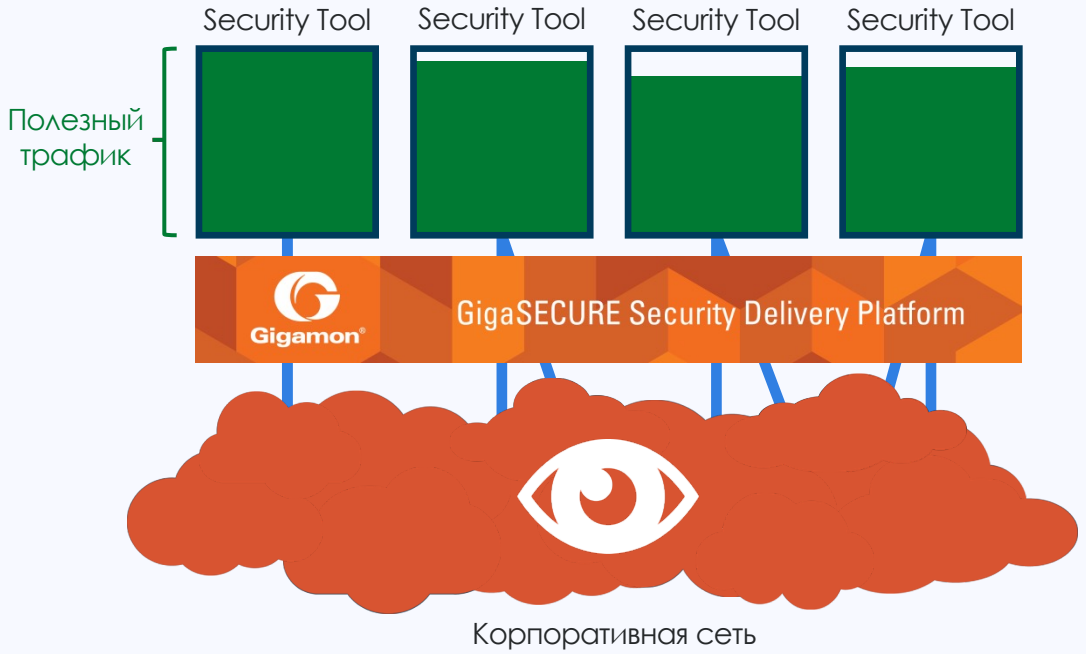
Как платформа влияет на ИБ

Подключение средств ИБ без Gigamon



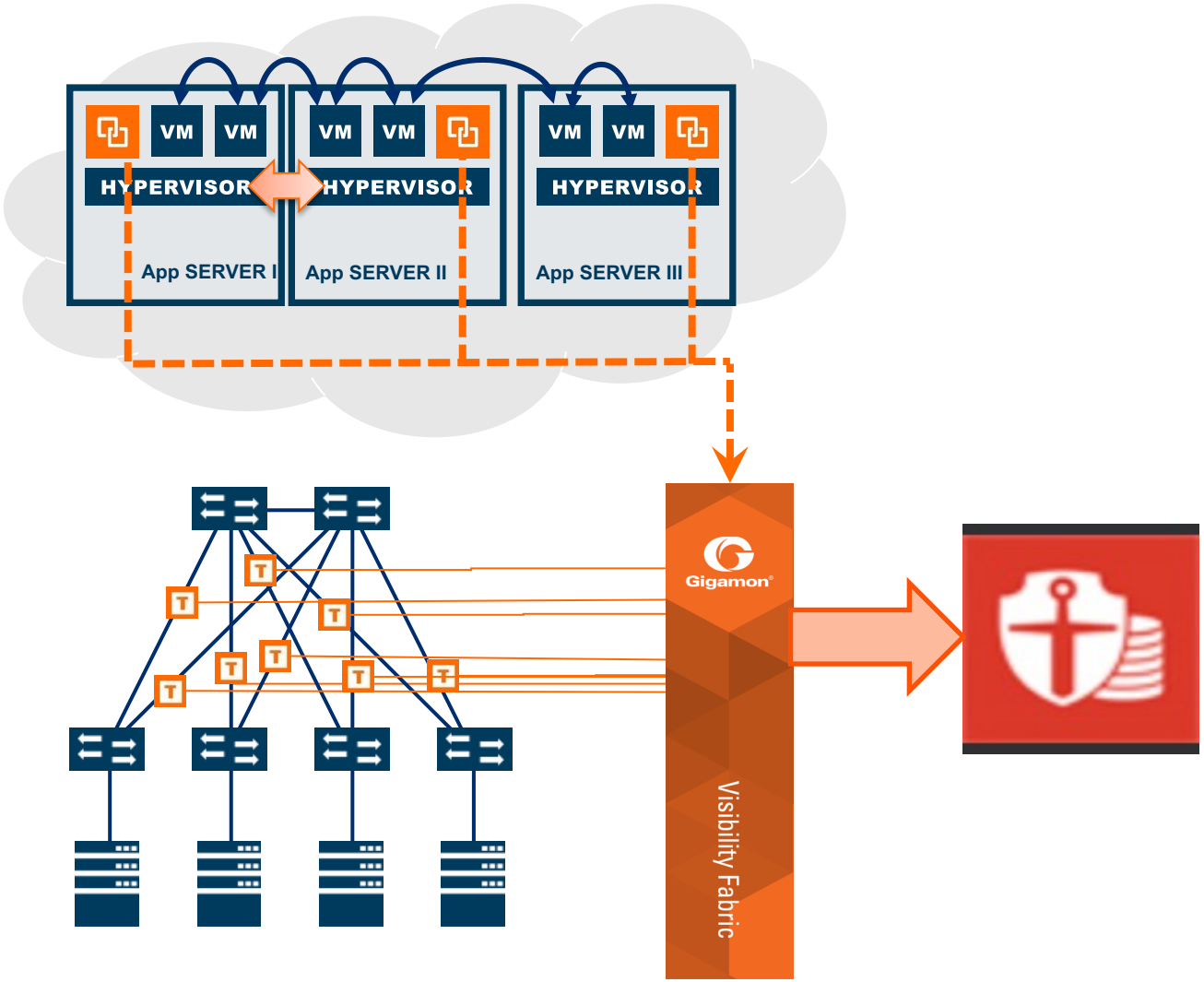
- ☒ Перегруженность систем ИБ «лишним» трафиком
- ☒ Высокая стоимость решения
- ☒ Снижение эффективности средств ИБ
- ☒ Проблемы с масштабированием

Подключение средств ИБ с Gigamon



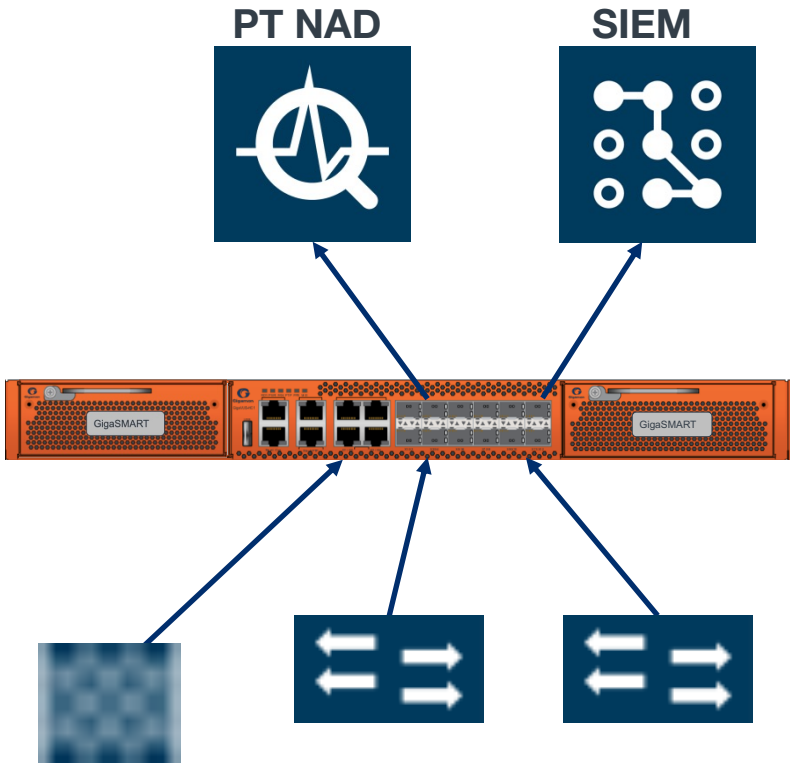
- ✓ Каждая система ИБ получает только нужный трафик
- ✓ Доступ к трафику из любой точки сети
- ✓ Повышение эффективности инструментов ИБ
- ✓ Снижение OPEX

Gigamon + Гарда преимущества



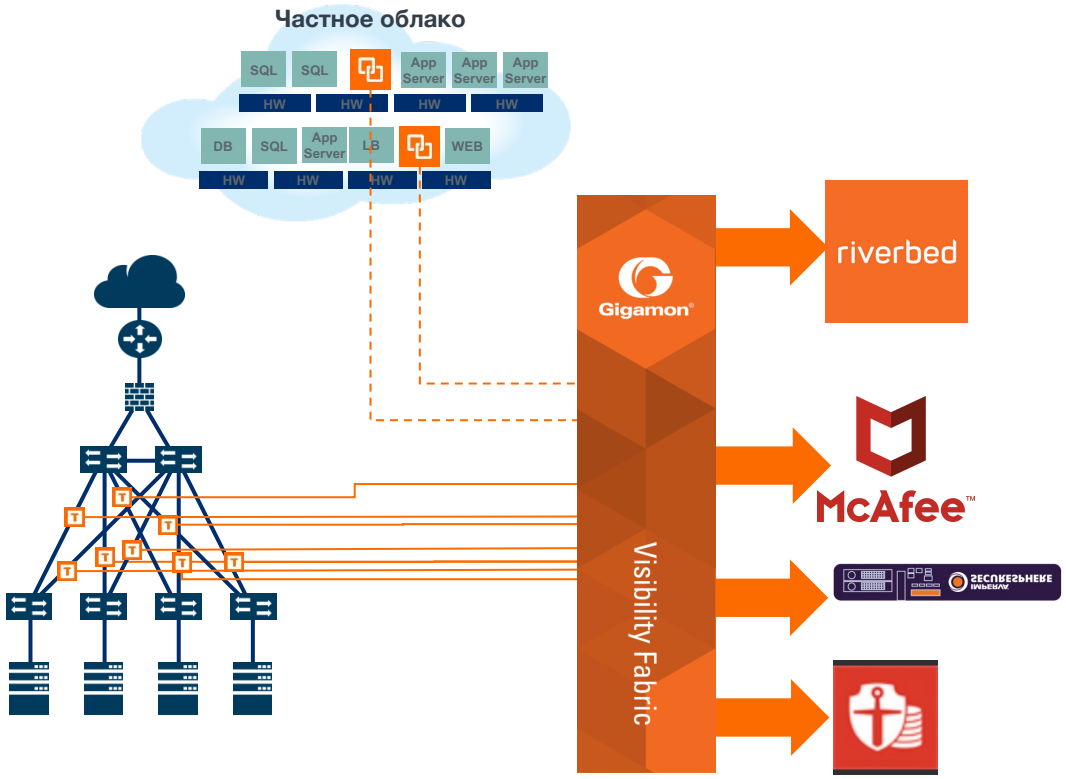
- ✓ Gigamon решает проблему предоставления доступа Гарда БД к трафику традиционной и\или гибридной сети.
- ✓ Фильтрация копии трафика и удаление дублированных пакетов снижают нагрузку на оборудование Гарда БД.
- ✓ Упрощается процесс расширения и модернизации Гарда БД.
- ✓ В несколько раз уменьшается скорость внедрения.
- ✓ Готовность быстро адаптироваться к изменениям в сетевой архитектуре.
- ✓ Нулевое влияние на сетевую инфраструктуру.
- ✓ Снижение затрат на внедрение и эксплуатацию решения

Gigamon + PT NAD и SIEM



- ✓ Консолидация копии трафика от нескольких источников, повышает эффективность работы получателей т.к. они видят «всю картину целиком»
- ✓ Фильтрацией и дедубликацией уменьшили объемы подаваемого трафика на PT NAD в 5 раз. И он получает только нужный трафик, ничего лишнего.
- ✓ В ходе проекта направили Netflow на SIEM, и перестали генерировать его на сетевых устройствах тем самым снизили нагрузку на сеть.
- ✓ Внедрение пакетного брокера не привело к увеличению бюджета проекта!!!
- ✓ Заказчик планирует в ближайшее время перевести подключение DBF и DLP на пакетные брокеры.

Пример решения в крупном банке

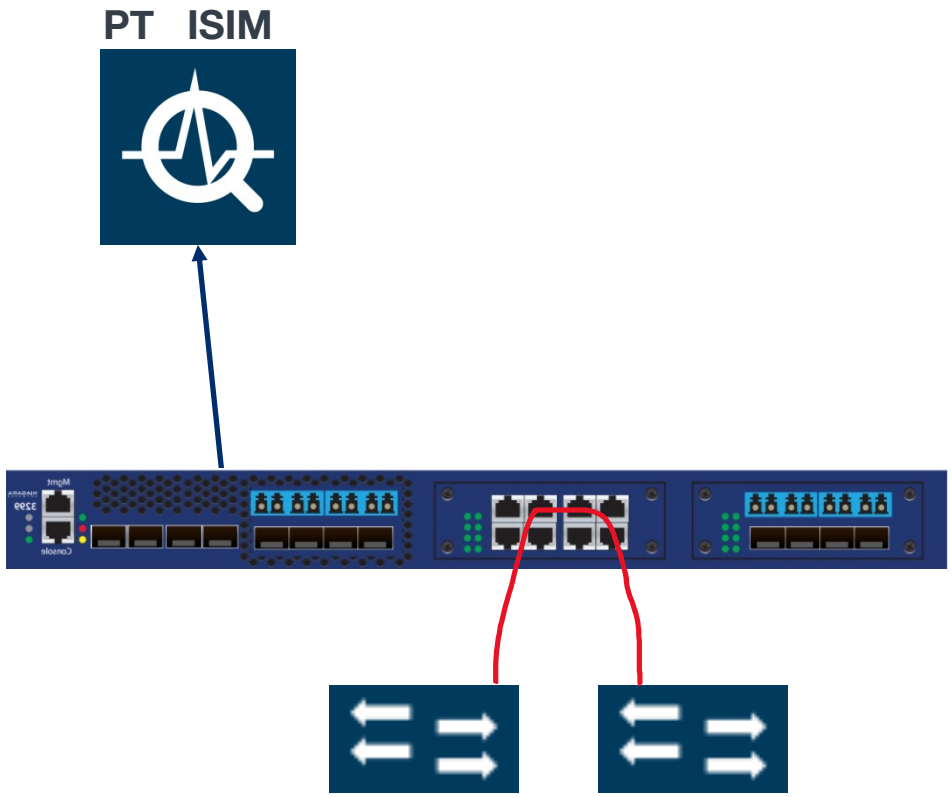


- Необходимо минимизировать дополнительную нагрузку на инфраструктуру виртуализации, возникающую при копировании трафика
- Сложная архитектура сети не позволяет осуществлять централизованный мониторинг. Что существенно увеличивает стоимость средств ИБ и мониторинга ИТ
- Получателям необходим одновременный доступ к трафику от виртуальных машин и проходящий по традиционной сети.

Полученный результат с Gigamon:

- ☑ Снижение объемов отправляемой копии трафика из виртуальной среды на 60%.
- ☑ Централизация мониторинга позволила снизить затраты на соответствующие платформы и повысить их эффективность работы
- ☑ Консолидация копий трафика из нескольких датацентров и виртуальной инфраструктуры позволило системам ИБ и ИТ эффективно контролировать сеть и коррелировать события происходящие в разных частях сети.

Решения для ИБ в АСУТП



Для подключения средств безопасности АСУ ТП часто приходится получить копию трафика от десятков источников, консолидировать ее для одного получателя, а так же исключить возможность передачи трафика обратно в сетевой канал. Для этих целей лучшее решение на рынке:

- ✓ Niagara Networks модель 3299 – идеальное сочетание медного TAP и агрегатора с привлекательной ценой
- ✓ Может принимать трафик от SPAN и выполнять функции TAP
- ✓ Позволяет получить копию трафика когда не доступен SPAN порт. Копирует трафик из сетевого кабеля.
- ✓ Обратная передача трафика исключена – заменяет датадиод
- ✓ Позволяет встать в разрыв до 12 медных соединений, выполнить агрегацию копии трафика и передать через 1-4 10G порта.
- ✓ Есть возможность фильтрации копии трафика

Как Gigamon меняет показатели бизнеса

ЗАЩИЩЕННОСТЬ И ПРОИЗВОДИТЕЛЬНОСТЬ СЕТИ

70% ↓
Снижение количества ложных срабатываний

50% ↓
Снижение времени простоя

ВИДИМОСТЬ И ЗАТРАТЫ НА СЕТЬ

75% ↑
Повышение доступности сети для средств мониторинга и ИБ

50% ↓
Снижение затрат

СКОРОСТЬ АДАПТАЦИИ И СЛОЖНОСТЬ БИЗНЕСА

РОСТ ↑
Упрощает адаптацию бизнеса к новым требованиям

СНИЖЕНИЕ ↓
Снижает сложность архитектуры сети

“ Клиенты ESG в интервью и беседах отмечают что платформа Gigamon – это критический инструмент для успешного бизнеса в наши дни. ”

NETWELL

Благодарю за внимание