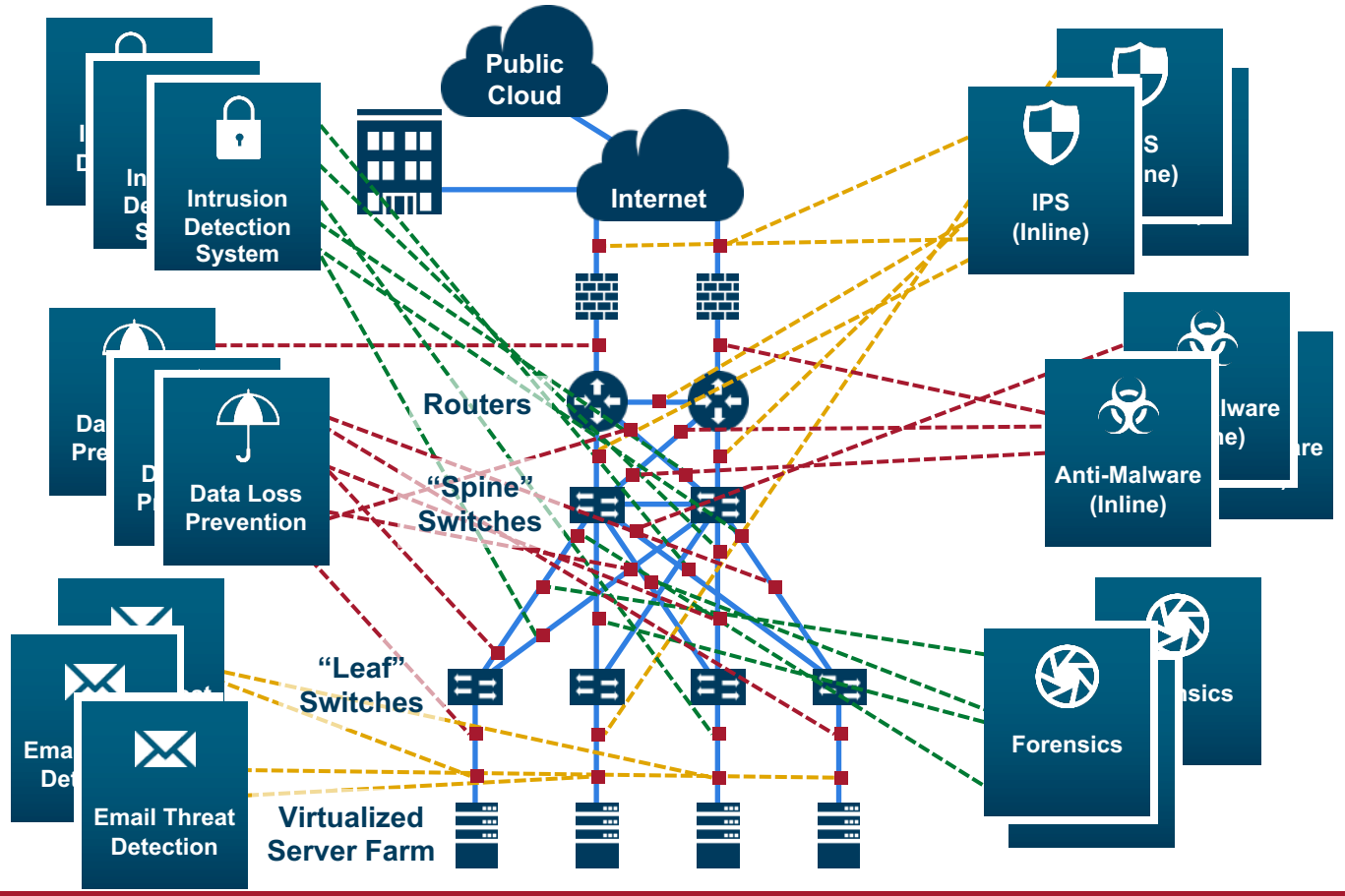
Рынок для продуктов зеркалирования: как идентифицировать потенциального заказчика и продать ему высокомаржинальный продукт.

Александр Грачев

BDM по продуктам зеркалирования трафика

Netwell

Подключение ИБ «бесплатными» средствами

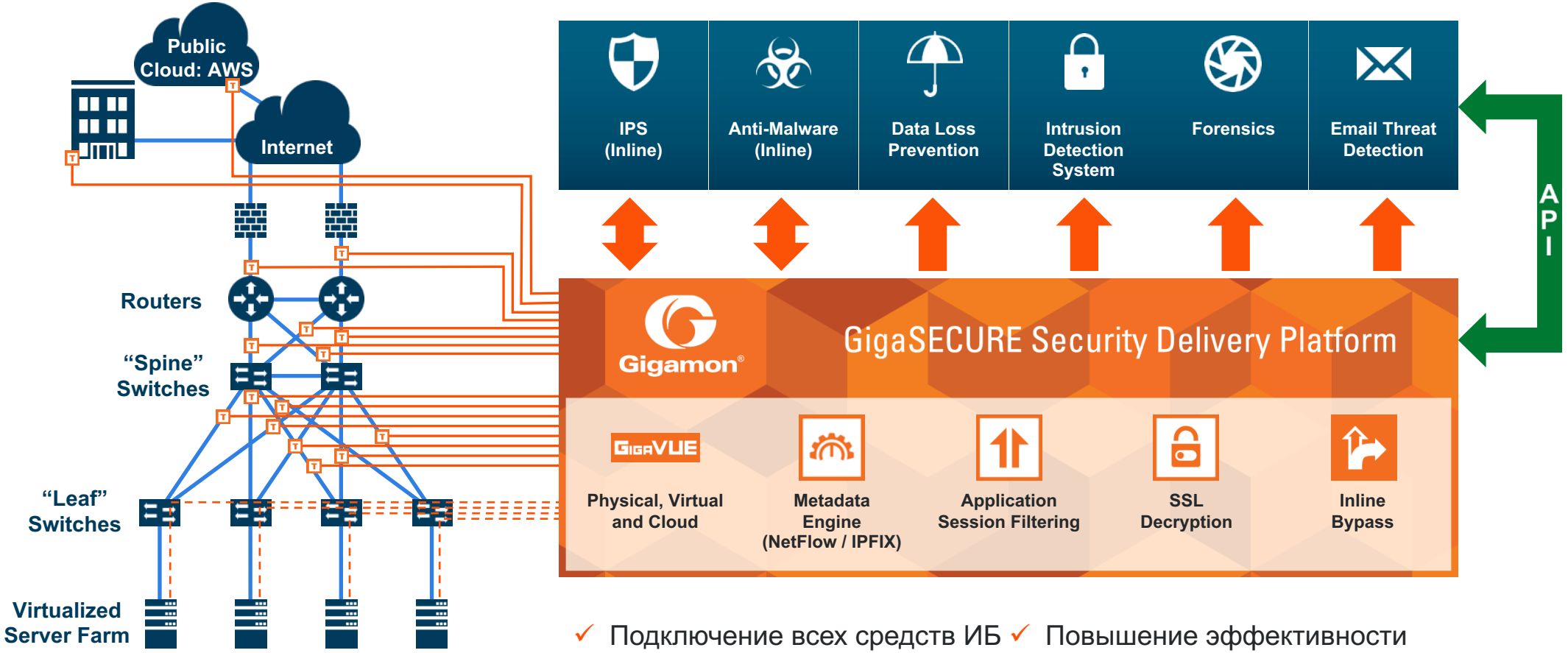


- Перегруженность систем ИБ «лишним» трафиком
- Высокая стоимость решения
- Трудность реализации и эксплуатации
- Проблемы с масштабированием и расширением
- Ложные срабатывания
- Проблемы с шифрованным трафиком

Плохая архитектура снижает эффективность средств ИБ!

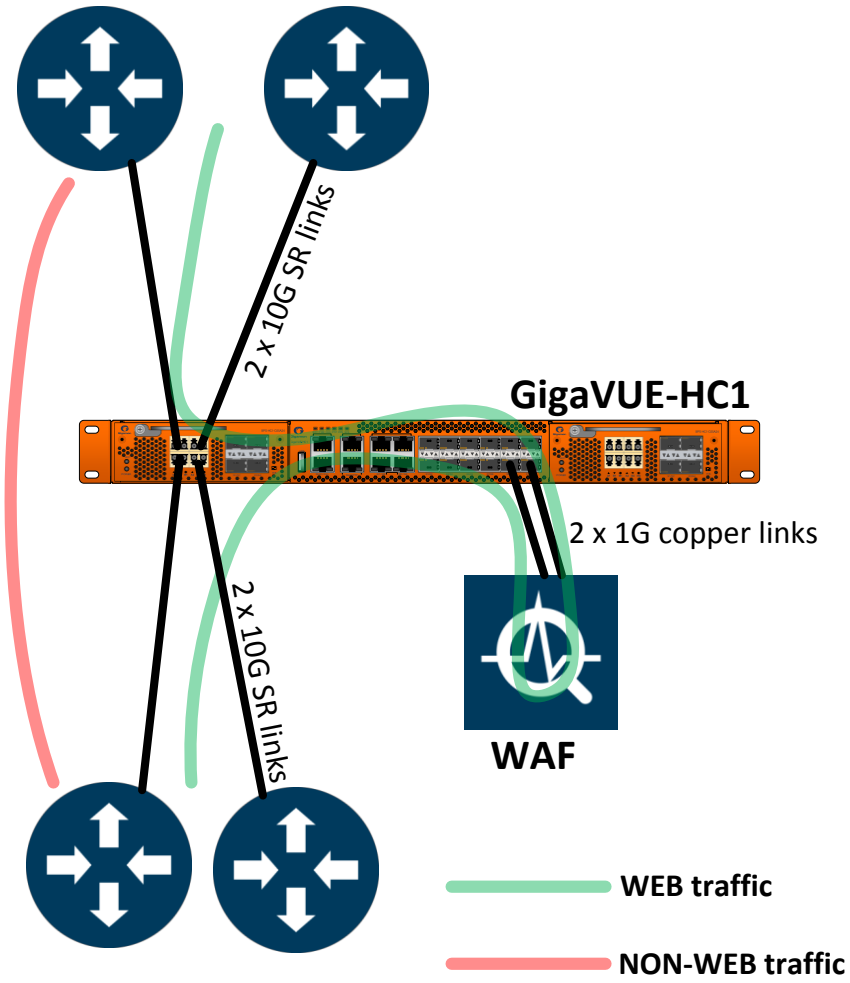
Security Delivery Platform: “Видеть все”

ОСНОВНОЙ ЭЛЕМЕНТ В СТРУКТУРЕ КИБЕРБЕЗОПАСНОСТИ



- ✓ Подключение всех средств ИБ
- ✓ Уменьшение дополнительных точек отказа в сети
- ✓ Повышение эффективности средств ИБ
- ✓ Снижение OPEX

Подключение WAF в гос. заказчике



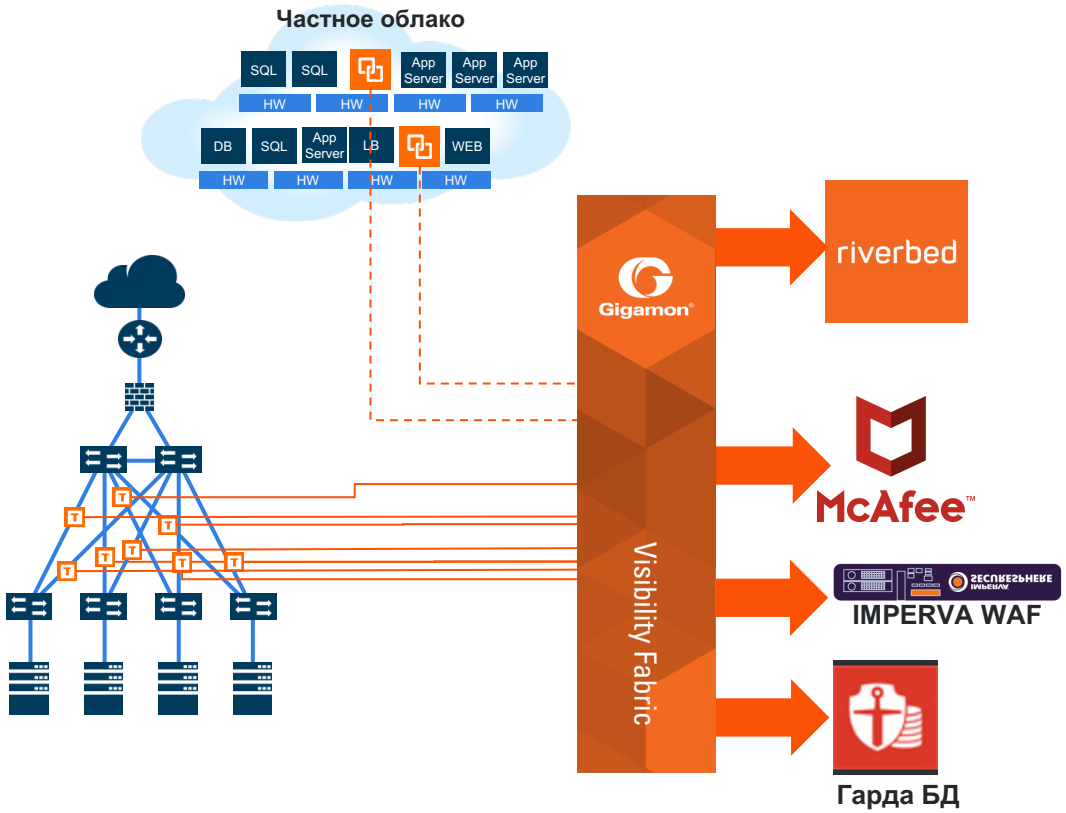
Задачи проекта:

- Подключить WAF Imperva через ByPass в сегмент сети.
- Снизить стоимость решения.
- Стоимость решения без ByPass брокера ~150К $

Решение:

- ☑ Подключение 1G WAF Imperva(~50K$) через ByPass брокер (~40K$)
- ☑ Стоимость проекта снижена на 40%
- ☑ Возможность подключение к ByPass брокеру других средств мониторинга и ИБ

Пример решения в Большом Банке



Решаемые проблемы:

- 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.

Энтерпрайз заказчик

Проблемы

- Элементы баз данных постоянно мигрируют между 2мя датацентрами
- Часть нужного трафика в виртуальных средах VMware и Nutanix
- Установить сенсоры DBF в 20 серверных каждого датацентра – неприемлемо дорого
- Использование SPAN портов приводит к частым авариям на сети

Решение

- Средства копирования трафика из виртуальной среды GigaVUE-VM и V-series
- Оптические TAP
- Кластер из пакетных брокеров TA и HC серии

Результат

- Повышена стабильность работы сети за счет ухода от SPAN портов
- Трафик из виртуальной среды доставляется на центральный сенсор DBF
- Снижены финансовые затраты на внедрение DBF на 60%
- Платформа Gigamon используется для подключения других средств ИБ и ИТ

Пример Банк (DLP)

Задача

- Получить копию трафика в двух датацентрах
- Не использовать SPAN, т.к. его использование вызывало аварии на сети
- Передать копию только e-mail трафика на DLP MCAFEE
- Удалить дублированные пакеты

Решение

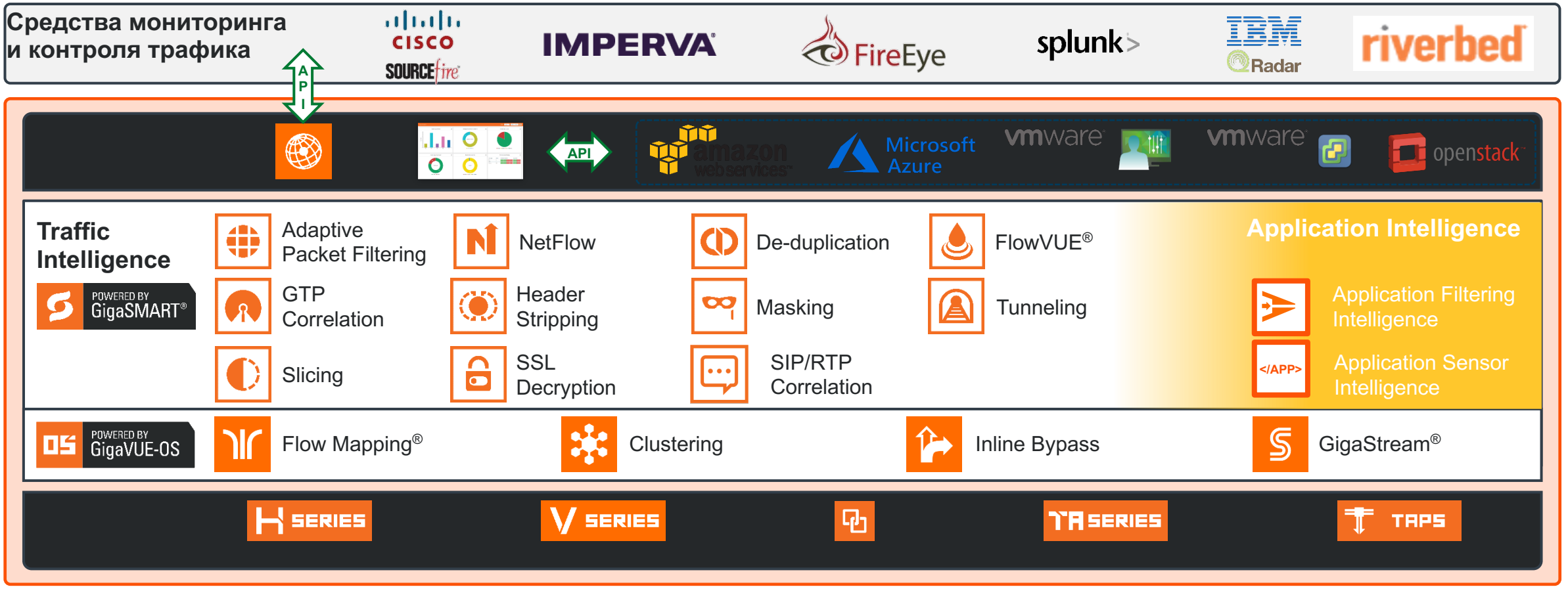
- Медные и оптические TAP
- 2 устройства H-серии

Результат

- Повышена стабильность работы сети за счет ухода от SPAN портов
- Прекращены ложные срабатывания, вызванные дублированными пакетами
- Снижение объемов получаемого DLP трафика на 60%, за счет фильтрации
- Подключение других средств ИБ и траблшутинга ИТ

Перераспределение расходов…

Платформа Gigamon – лидер рынка



Любая сеть

Датацентры и частное облако | Публичное облако | Сеть сервис провайдера | Удаленные датацентры

Почему Gigamon лидер рынка

- Фокусированность на продукте.
  - ✓ Gigamon не отвлекается на другие продукты и следует запросу рынка в развитии своего портфолио.
- Интенсивное развитие платформы.
  - ✓ Своевременная разработка новых моделей и функций.
  - ✓ От 100 до 200 новых функций внедряется ежегодно, многие из них входят в состав базового функционала.
- Высокая надежность оборудования.
  - ✓ Несколько крупнейших заказчиков признали Gigamon самым надежным решением на сети
- Самое большое портфолио на рынке зеркалирования
  - ✓ Наибольшее покрытие известных виртуальных платформ
  - ✓ Наибольшее количество инструментов модификации трафика.
  - ✓ Обширный набор многофункционального оборудования и TAP.

Драйверы развития платформы **Gigamon**

- Платформа зеркалирования одна из самых быстрорастущих решений на сети.
- Решения анализирующие трафика из разных мест сети: NBA, NPM, APM, SIEM – неизбежно потребуют наличие платформы зеркалирования. (иногда об этом задумываются после их закупки)
- Внедрение новых средств мониторинга и платформ ИБ, а так же масштабирование существующих.
- Рост трафика общего трафика сети, модернизация сетевой инфраструктуры (1G -> 10G ->100G), миграция в облако, появление новых приложений - заставляют адаптировать инструменты ИБ и ИТ для работы в новых условиях.

Развитие платформы Gigamon в сети

Соединяем кубики

SIEM: Splunk, LogRhythm, IBM
APM: Riverbed, NetScout
APT: FireEye
IPS: Cisco, PaloAlto, Fortinet
WAF: Imperva
DBF: **Гарда**

Почему Gigamon лидер рынка

- Фокусированность на продукте.
  - ✓ Gigamon не отвлекается на другие продукты и следует запросу рынка в развитии своего портфолио.
- Интенсивное развитие платформы.
  - ✓ Своевременная разработка новых моделей и функций.
  - ✓ От 100 до 200 новых функций внедряется ежегодно, многие из них входят в состав базового функционала.
- Высокая надежность оборудования.
  - ✓ Несколько крупнейших заказчиков признали Gigamon самым надежным решением на сети
- Самое большое портфолио на рынке зеркалирования
  - ✓ Наибольшее покрытие известных виртуальных платформ
  - ✓ Наибольшее количество инструментов модификации трафика.
  - ✓ Обширный набор многофункционального оборудования и TAP.

VISIBILITY MATTERS