



Решения для обеспечения безопасности виртуальных сетей, частных и публичных облаков

Александр Грачев

Старший инженер-консультант





See what matters.TM

Gigamon Visibility Platform provides pervasive visibility into data in motion across your entire network, enabling stronger security and network performance.

- Основана в 2004
- Штаб-квартира: Санта Клара, США
- Офисы в 20 странах
- 700 сотрудников на 12.01.2018
- CEO: Paul Hooper
- Более 2,500+ заказчиков
- Рынки: Гос Учреждения, Телеком, Финансы, Здравоохранение, Крупные Розничные Сети, Транспорт, Нефть&Газ, Технологические компании
- Оборот за 2016 год \$320М, +40% YoY

Statistics as of December 2016

Присутствие Gigamon на глобальном рынке

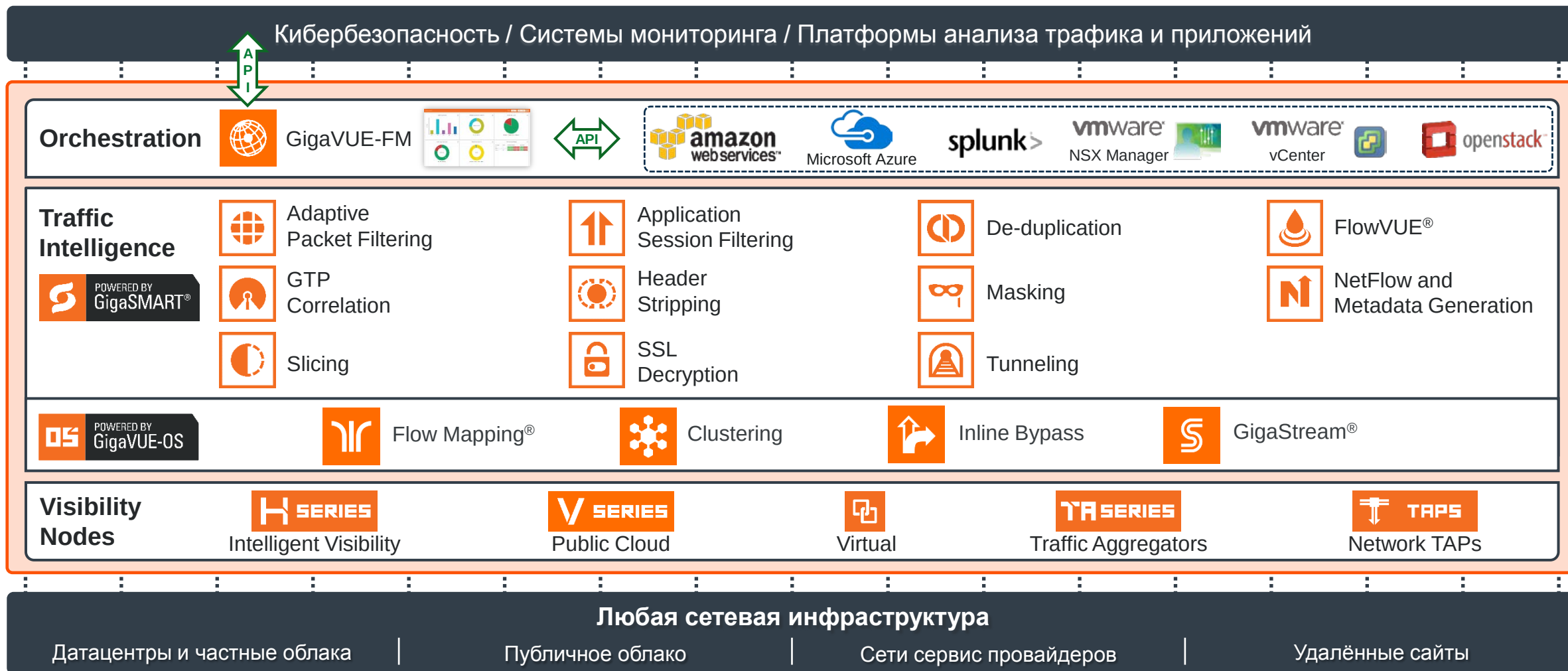


Fortune 100 and 1000 statistics from FY 16-Q3
Top 50 Banks in the World." <http://www.relbanks.com/worlds-top-banks/assets> Banks around the World. June 30, 2015. Web.
Laura Lorenzetti "The 10 biggest health-care companies in the Fortune 500." <https://gigamon.my.salesforce.com/00O14000008ef5s> Fortune. June 20, 2015. Web.
Pablo Erbar "20 Largest Stock Exchanges in the World." <http://www.insidermonkey.com/blog/trading-places-the-20-largest-stock-exchanges-in-the-world-335310/>
Insider Monkey. November 11 2014. Web.

Liyan Chen "The World's Largest Tech Companies: Apple Beats Samsung, Microsoft, Google." <http://www.forbes.com/sites/liyanchen/2015/05/11/the-worlds-largest-tech-companies-apple-beats-samsung-microsoft-google/> Forbes. May 11, 2015. Web.
Kantar Retail "Top 100 Retailers Chart 2015." <https://nrf.com/2015/top100-table> National Retail Federation. 2015. Web.
Liyan Chen "The World's Largest Telecom Companies: China Mobile Beats Verizon, AT&T Again." <http://www.forbes.com/pictures/fji45fkkh/china-mobile/> Forbes.
June 1, 2015. Web.

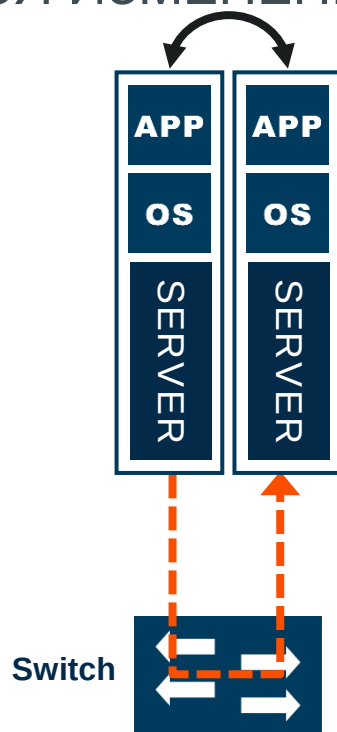
Портфолио

See What Matters.™



Виртуализация объектов мониторинга

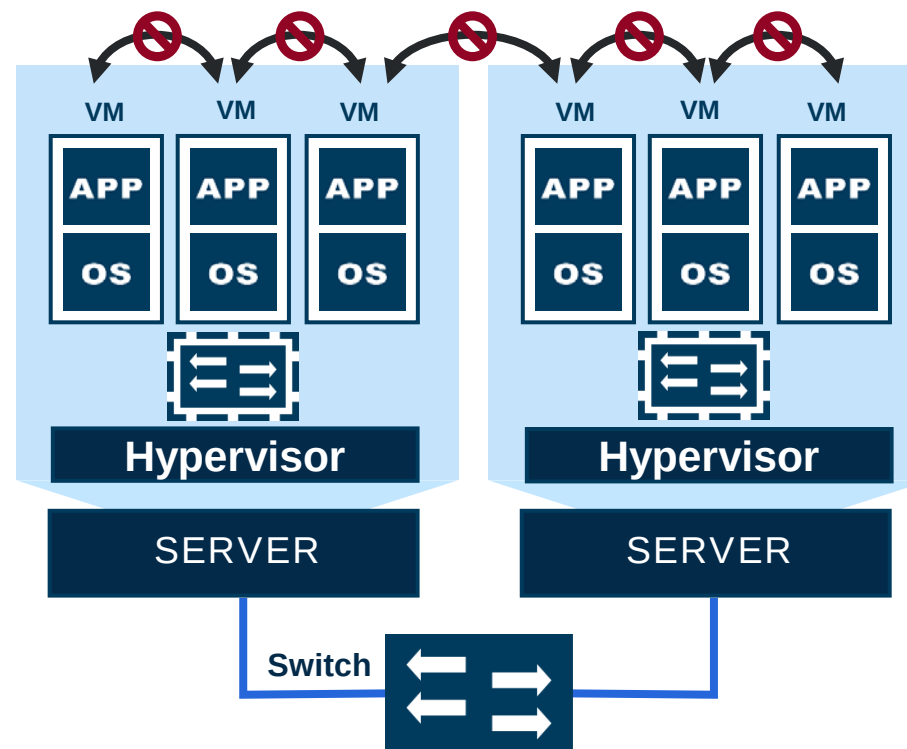
ТРЕБУЕТСЯ ИЗМЕНЕНИЕ ПОДХОДА



Традиционный подход

- SPAN порты
- Сетевые сплиттеры

ВИРТУАЛИЗАЦИЯ



Проблемы копирования трафика VM традиционным способом

- «Слепые зоны» - трафик VM-VM внутри одного хоста
- «Слепые зоны» - трафик VM-VM между блейдами Blade Center

ИТ Безопасность, ИТ мониторинг и Контроль работы приложений нарушаются!!!

Необходим универсальный инструмент для анализа трафика виртуально среды

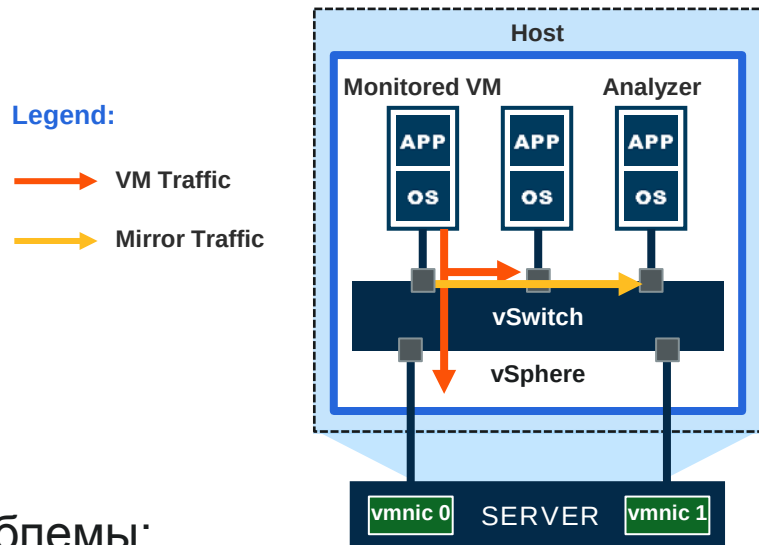
- ▶ Мониторинг работы приложений  Application Performance Management
- ▶ Управление клиентским опытом  Customer Experience Management
- ▶ Анти-фрод  Voice Analysis (SIP)
- ▶ Кибербезопасность  Intrusion Detection (IDS)
Intrusion Prevention (IPS)
Data Loss Prevention (DLP)
Forensics and Analytics (SIEM)

Всем этим платформам нужна копия трафика сети!

Мониторинг виртуальных объектов

ВОЗМОЖНЫЕ РЕШЕНИЯ И ПРОБЛЕМЫ

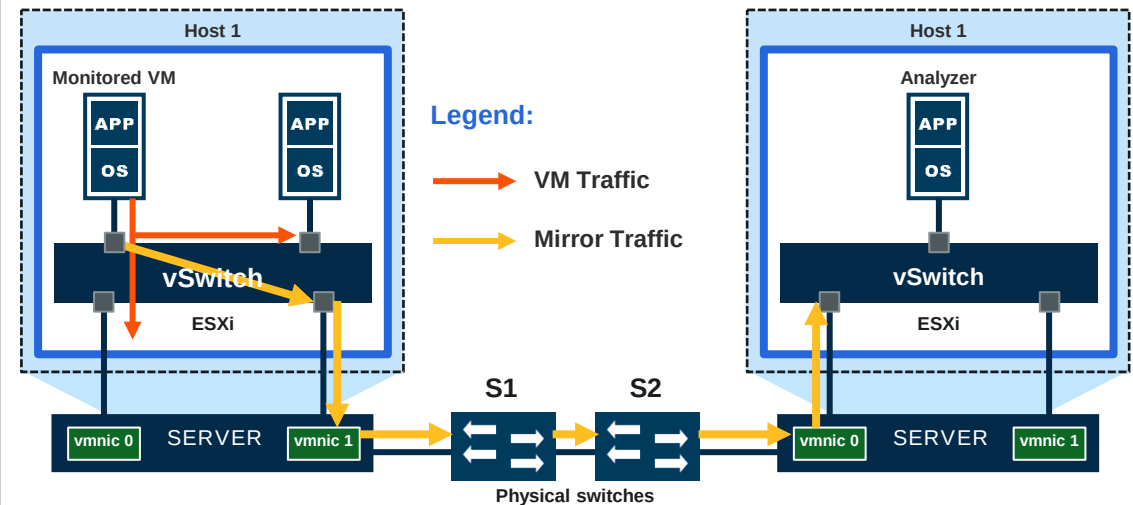
Распределенная архитектура



Проблемы:

- Как подключать несколько получателей?
- Увеличение нагрузки на виртуальную среду.
- Проблемы сохранения мониторинга при миграции объекта мониторинг

Централизованная архитектура



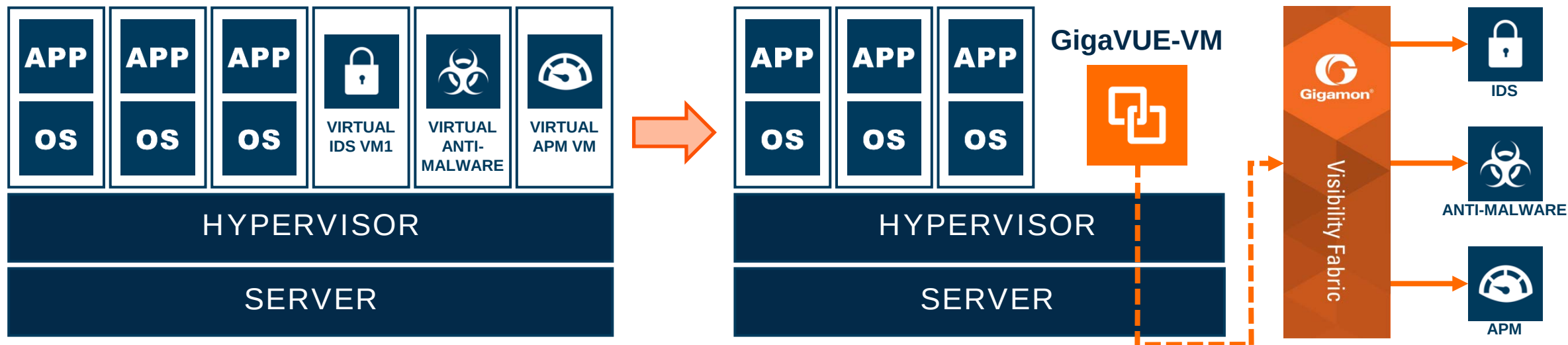
Проблемы:

- Как подключать несколько получателей?
- Увеличение нагрузки на виртуальную среду.
- Проблемы сохранения мониторинга при миграции объекта мониторинг

Почему важно контролировать виртуальную среду?

5 ПРОБЛЕМ МОНИТОРИНГА ВИРТУАЛЬНЫХ ОБЪЕКТОВ

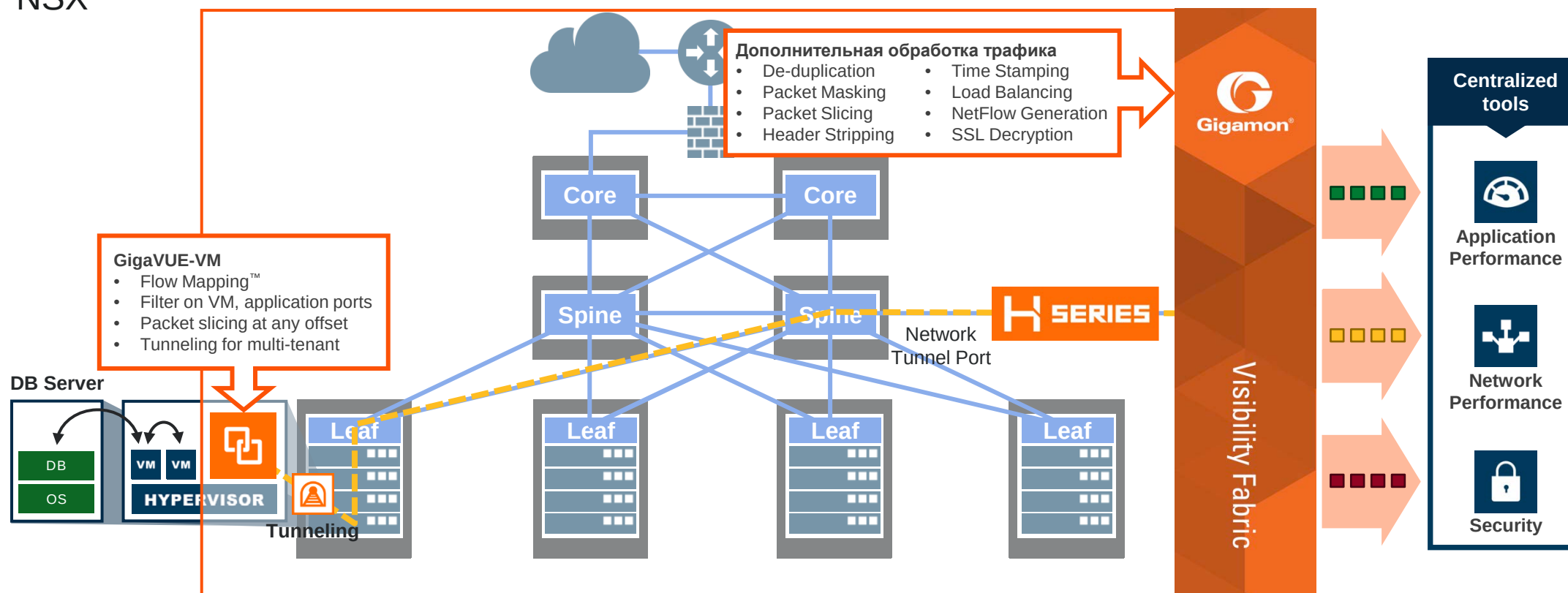
1. «Слепые зоны» - трафик между VM не проходит через физическую среду.
2. Автоматическая миграция VM между гипервизорами.
3. Увеличение количества объектов мониторинга.
4. Миграция объектов мониторинга в виртуальную среду, требует изменения систем мониторинга.
5. Создание новых VM требующих мониторинга.



GigaVUE-VM – Решение для виртуализации

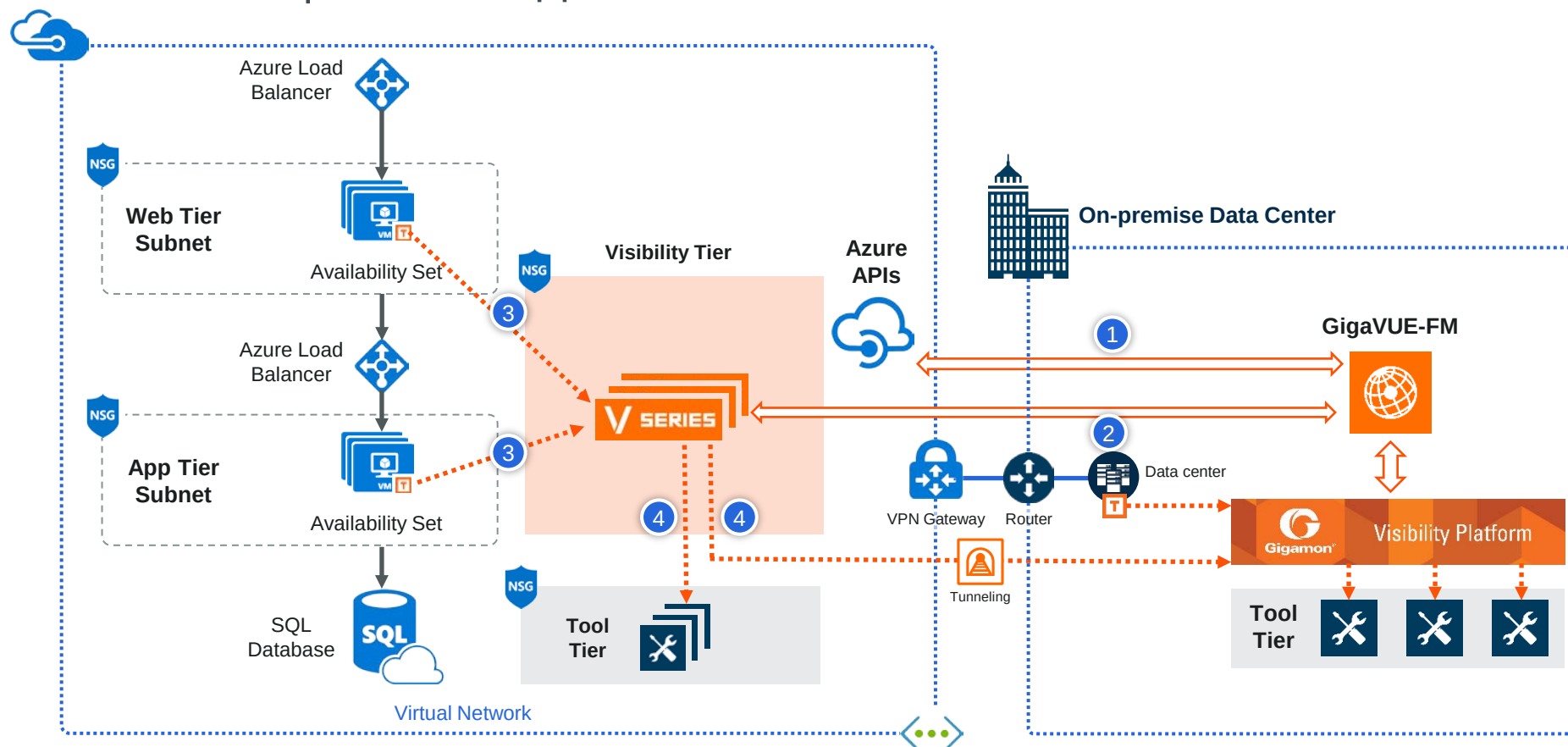
РАСШИРЕНИЕ ПЛАТФОРМЫ КОНТРОЛЯ ТРАФИКА В ВИРТУАЛЬНОЙ СРЕДЫ

- Небольшой размер виртуальной машины
- Работа виртуальными свичами VM Ware ESX и NSX
- Передача на платформу мониторинга только полезного трафика
- Работа с гипервизорами KVM



Решение для MS Azure

ОПТИМИЗАЦИЯ РАСХОДОВ В КИБЕРБЕЗОПАСНОСТЬ



- 1 Интеграция с Azure API
- 2 Платформа копирования трафика
- 3 Копия трафика виртуальных машин
- 4 Агрегирование трафика, его фильтрация и отправка получателям

Преимущества решения

КЛЮЧЕВОЕ ЗВЕНО МОНИТОРИНГА ВИРТУАЛЬНО СРЕДЫ

- Доступ ко всему трафику виртуальной среды.
- Автоматическая миграция политик мониторинга вместе с VM-объектом мониторинга.
- Фильтрация и оптимизация трафика перед отправкой в физическую среду.
 - Фильтрация по L3-L4 параметрам, для выделения нужного трафика
 - Обрезка Payload для снижения объемов передаваемого трафика
- Поддержка VM Ware ESX 5.1 и выше
 - Поддержка VDS, VSS, Cisco Nexus 1000v, NSX
 - Интеграция с несколькими vCenter
- Поддержка KVM Open stack, MS Azure, AWS

VISIBILITY
MATTERS

