

Security Delivery Platform – *необходимый* элемент инфраструктуры ИБ

необходимый элемент инфраструктуры ИБ



Безопасность каждой компании под угрозой

МНОГИЕ ИЗВЕСТНЫЕ БРЕНДЫ В РАЗНЫХ ОТРАСЛЯХ ЭКОНОМИКИ БЫЛИ УСПЕШНО «ВЗЛОМАНЫ»



Money. [“Data Breach Tracker: All the Major Companies That Have Been Hacked”](#) Март 18, 2015.

Информационная безопасность в цифрах

MARKET SIZE

Worldwide spending on information security will reach **\$75 billion for 2015**

The global cybersecurity market is expected to be **\$170 billion by 2020**

FEDERAL SPENDING

Demand for Information Security Products & Services: **\$8.6b in 2015**
\$11b in 2020

CYBER CRIME





Cyber-attacks are **costing** businesses **\$400 to \$500 billion a year**

COST PER BREACH

AVERAGE BY COUNTRY per record

| | |
|-------------------------------------------------------------------------------------|----------------------|
|  | U.S. \$217 |
|  | Germany \$211 |
|  | India \$56 |
|  | Brazil \$78 |

AVERAGE BY INDUSTRY per record

| | |
|---------------------------------------------------------------------------------------|------------------------------|
|  | Healthcare: \$363 |
|  | Education: \$300 |
|  | Transportation: \$121 |
|  | Public sector: \$68 |

FINANCIAL SERVICES

2015 U.S. financial services cybersecurity market will reach **\$9.5 billion** (largest non-government market)

GLOBAL MARKET

Asia-Pacific mobile security market is expected to garner **\$7.5+ billion by 2020**, one of the fastest growing sectors in the cybersecurity

SECURITY ANALYTICS

Hot areas for growth:

| | |
|----------------------------------|-------------|
| Security analytics / SIEM | ↑10% |
| Threat intelligence | ↑10% |
| Mobile security | ↑18% |
| Cloud security | ↑50% |

Традиционная модель безопасности



Защищенный
периметр

- Inside vs. outside
- Фокус на предотвращении

- Rule based
- Signature based



Простая
доверительная
модель

- Доверенное vs. недоверенное
- Корпоративные vs. личные устройства

- Размытие границ периметра
- BYOD



Статичные
средства
защиты

- Фиксированные зоны и периметры

- Мобильность пользователей, устройств, приложений



Традиционная модель безопасности

Более важно...

**САМА ПРИРОДА
КИБЕРАТАК
ИЗМЕНИЛАСЬ!**

- Rule based
- Signature based



-
- Размытие границ периметра
 - BYOD



-
- Мобильность пользователей, устройств, приложений



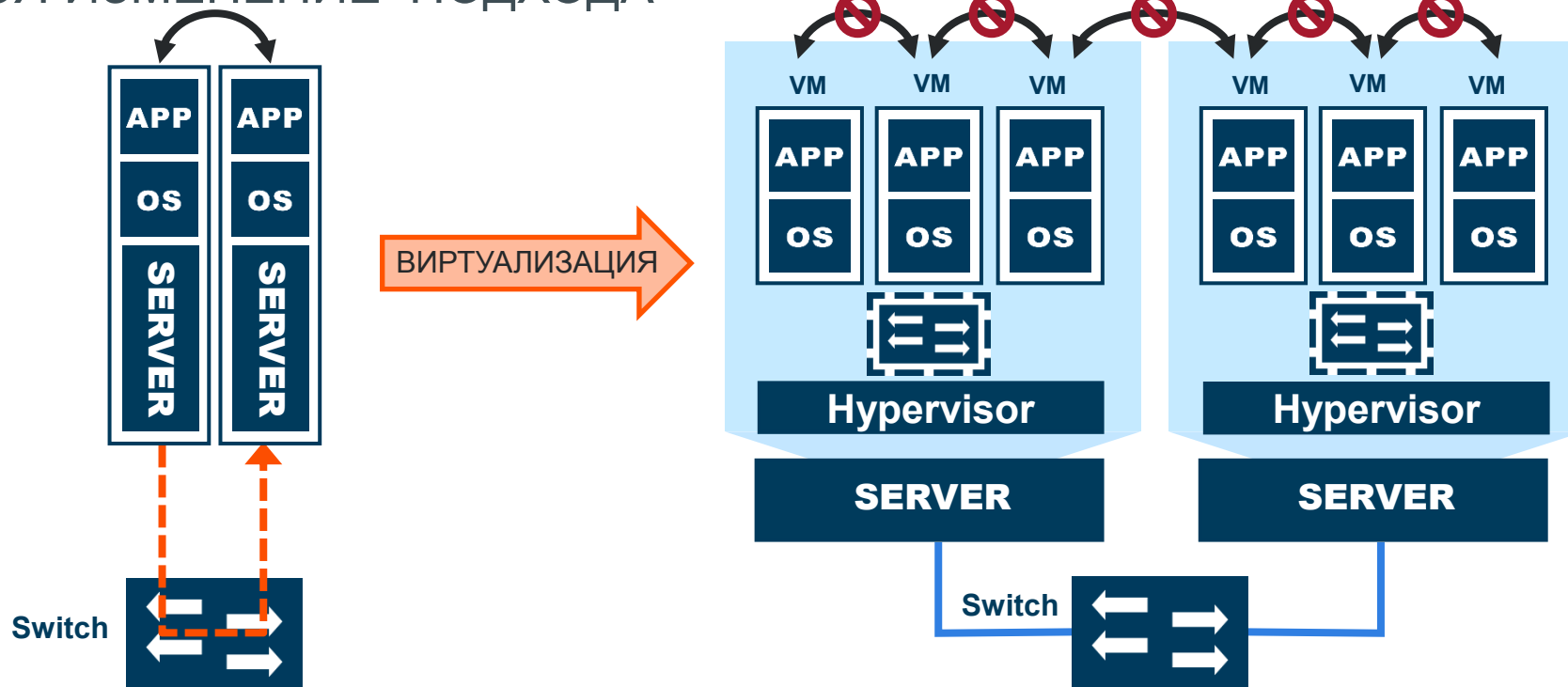
Анатомия сложной кибератаки



Во многих случаях система остается взломанной после атаки!

Внедрение виртуализации

ТРЕБУЕТСЯ ИЗМЕНЕНИЕ ПОДХОДА



- SPAN порты
- Сетевые сплиттеры

Потеря контроля над происходящим в виртуальной среде

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

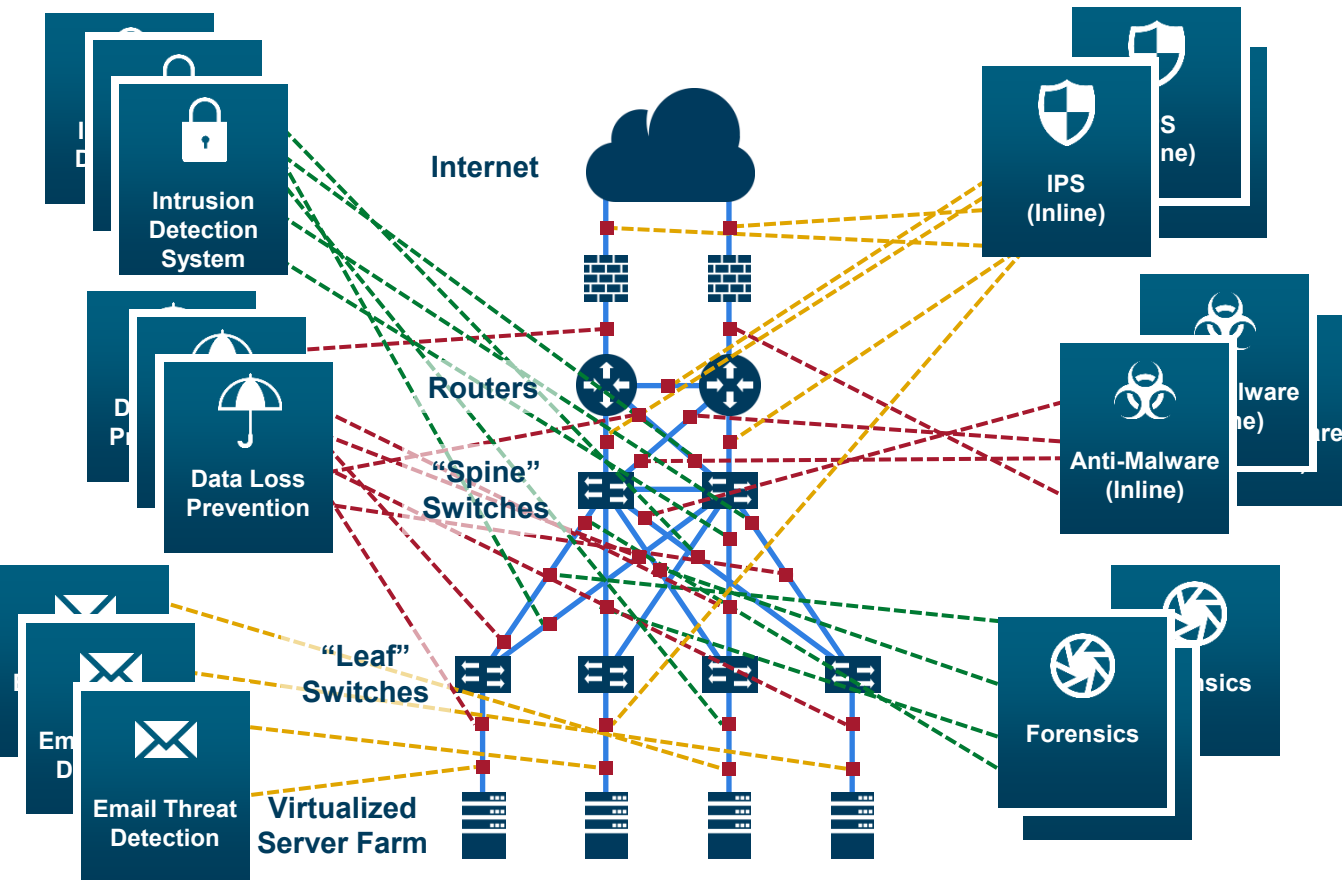
ИТ Безопасность и Контроль работы приложений нарушаются!!!

Идеальный Шторм: Требуется пересмотреть архитектуру ИБ



Внедрение систем ИБ

СРЕДСТВА ИБ ИМЕЮТ ПРОБЛЕМЫ С ДОСТУПОМ К НУЖНОМУ ТРАФИКУ



- Высокая стоимость решения
- Конкуренция за доступ к точкам включения
- Ассиметричная маршрутизация
- Проблемы с масштабированием и расширением
- Ложные срабатывания
- Проблемы с шифрованным трафиком
- Перегрузка средств ИБ

Время повысить эффективность ИБ инфраструктуры!

Платформа подключения средств ИБ

ДОСТУП К НУЖНОМУ ТРАФИКУ В ЛЮБЫХ СЕГМЕНТАХ СЕТИ

- Подключение **любых** средств ИБ/мониторинга/аналитики
- Оптимизация расходов
- Повышение эффективности средств ИБ
- Продление сроков эксплуатации решений
- Повышение надежности сети



Security Delivery Platform: Важное звено инфраструктуры ИБ

Требования к Visibility Fabric

ЧТО ДОЛЖНО ПОМОЧЬ РЕШИТЬ ПРОБЛЕМЫ ПОДКЛЮЧЕНИЯ СРЕДСТВ ИБ



- ✓ Создание множественных копий трафика
- ✓ Применение политик фильтрации в каждой копии
- ✓ Набор инструментов для «перехвата» трафика из физической и виртуально среды










- ✓ Наличие физической защиты для сетевых соединений
- ✓ Возможность пропускания через средства ИБ трафика по определённым политикам
- ✓ Подключения нескольких устройств ИБ одновременно

Все эти функции должны выполняться одним устройством

Дополнительные возможности платформы

МОДИФИКАЦИЯ КОПИЙ ТРАФИКА ДЛЯ УЛУЧШЕНИЯ РАБОТЫ СРЕДСТВ ИБ

| Название | Описание |
|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  De-duplication | <ul style="list-style-type: none">• Обеспечивает стабильную работу систем чувствительных к получению дублированных пакетов.• Снижение количества ложных срабатываний |
|  Header Stripping | <ul style="list-style-type: none">• Удалять выбранные заголовки из пакета, делая трафик доступным для анализа.• Позволять получателям трафика не тратить ресурсы на обработку икапсулированных пакетов. |
|  IP Tunneling | <ul style="list-style-type: none">• Терминация ERSPAN и GRE тоннелей для получения копий трафика из IP сети• Отправка копий трафика через GRE тоннель на удаленного получателя через IP сеть |
|  SSL Decryption | <ul style="list-style-type: none">• Дешифровка копий трафика SSL и TLS перед отправки их получателям• Снижение нагрузки на получателей трафика за счет отправки копий в расшифрованном виде. |
|  Генерирование NetFlow | <ul style="list-style-type: none">• Генерирование NetFlow версий 5, 9 и IPFIX, и отправка его на несколько коллекторов• Добавление мета-данных (URL, HTTP error codes, DNS info, аномалии HTTPS, User Names) |
|  Packet Slicing | <ul style="list-style-type: none">• Удаление конечной части пакета начиная с определяемого места.• Позволяет снизить объемы передаваемого трафика и предотвратить передачу user data |
|  Masking | <ul style="list-style-type: none">• Замена выбранных полей в пакете на нечитаемые символы• Защитить важную информацию (номера кредитных карт, телефонов и т.п.) для предотвращения несанкционированного ее использования |

Преимущества

БЫСТРОЕ ОБНАРУЖЕНИЕ, СНИЖЕНИЕ ПОТЕРЬ



- **Предоставление доступа к трафику сети для всех средств ИБ**
- **Устранение конкуренции за доступ к трафику**
- **Повышение отказоустойчивости сети:** обновление, расширение внедрение средств ИБ проходят без влияния на сеть.
- **Устраняет проблему слепых зон:** доступ к мобильному, шифрованному и виртуальному трафику
- **Повышение эффективности средств ИБ:** фильтрация копий трафика, NetFlow, дешифрация SSL... высвобождают ресурсы средств ИБ от подготовки трафика, и уменьшают кол-во ложных срабатываний
- **Оптимизация расходов на внедрение и использование средств ИБ за счет их оптимальной работы.**

Итог

▶ Информационная безопасность современных сетей движется от модели «предосторожности» к модели «обнаружения и реагирования»

▶ Новая модель требует контроль всей сети и внедрения большего количества активных и пассивных средств ИБ, практически во все участки сети

▶ Security Delivery Platform позволяет осуществить переход к новой модели ИБ с наименьшими затратами, при этом повысить эффективность существующих средств ИБ

Спасибо

