Построение эшелонированной защиты от DDoS-атак

Вадим Солдатенков, руководитель группы продуктов «Гарда Anti-DDoS»

DDoS-атаки

угроза, которая не исчезает

85% российских компаний подвергаются атакам не реже раза в год

2024 год

рост сложных мультивекторных атак

2024 год

увеличение количества атак на критическую инфраструктуру России

Ущерб репутации

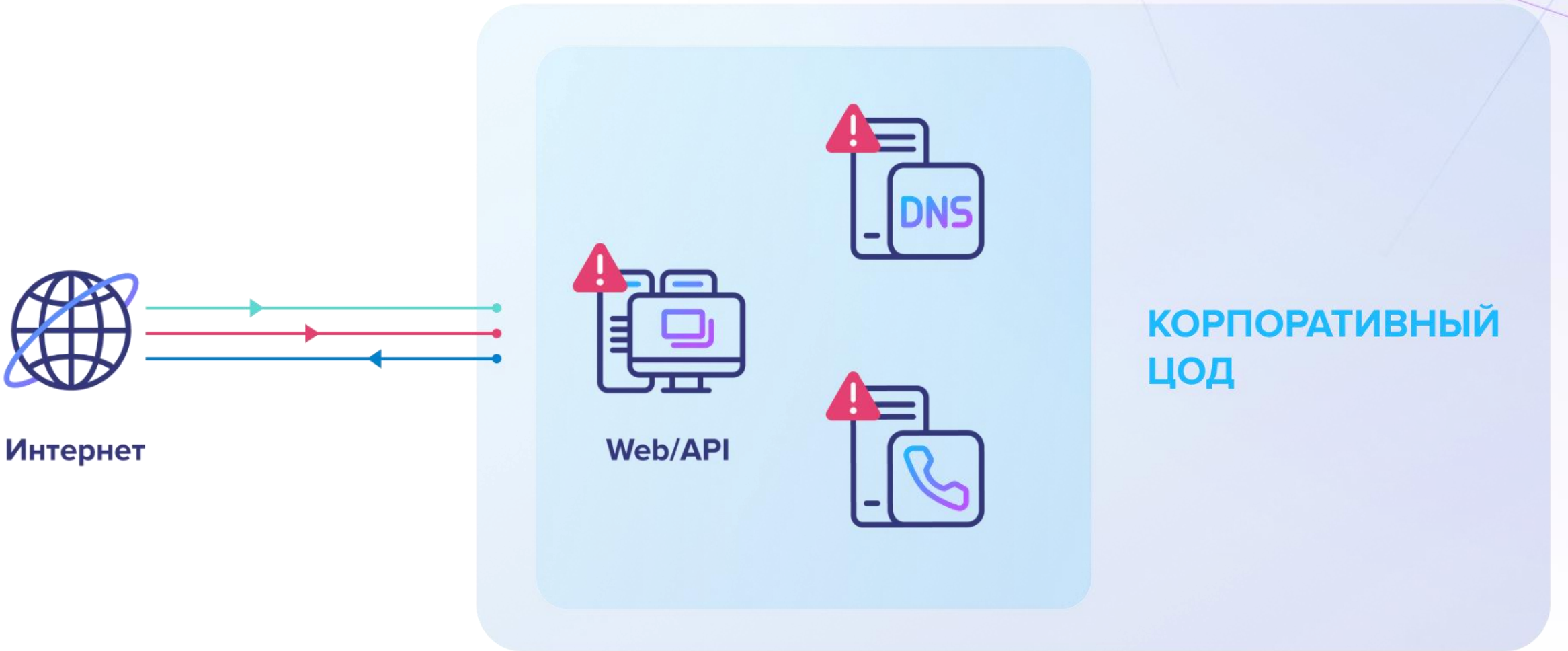
Недоступность сервисов для клиентов

Полная остановка бизнес-процессов

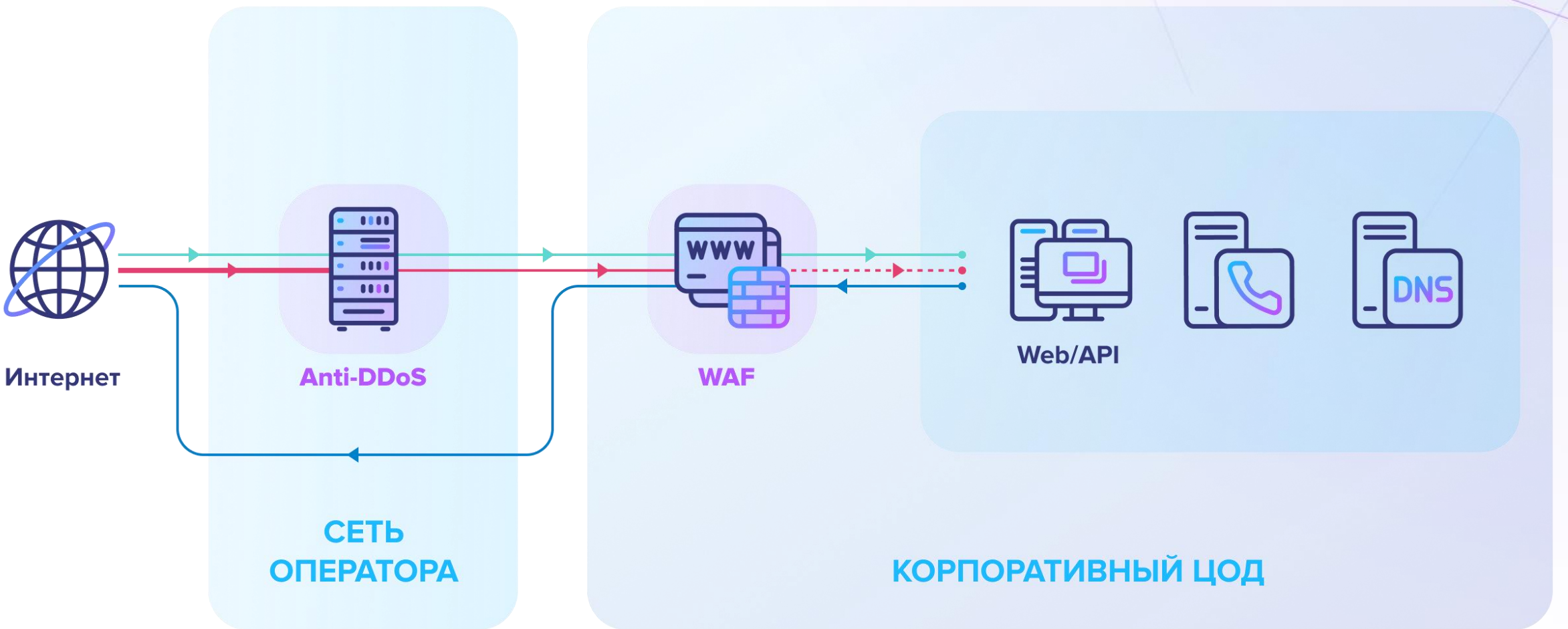
Кража данных под прикрытием DDoS-атаки

Финансовые потери из-за простоя

Защита от DDoS — одна из ключевых задач ИБ



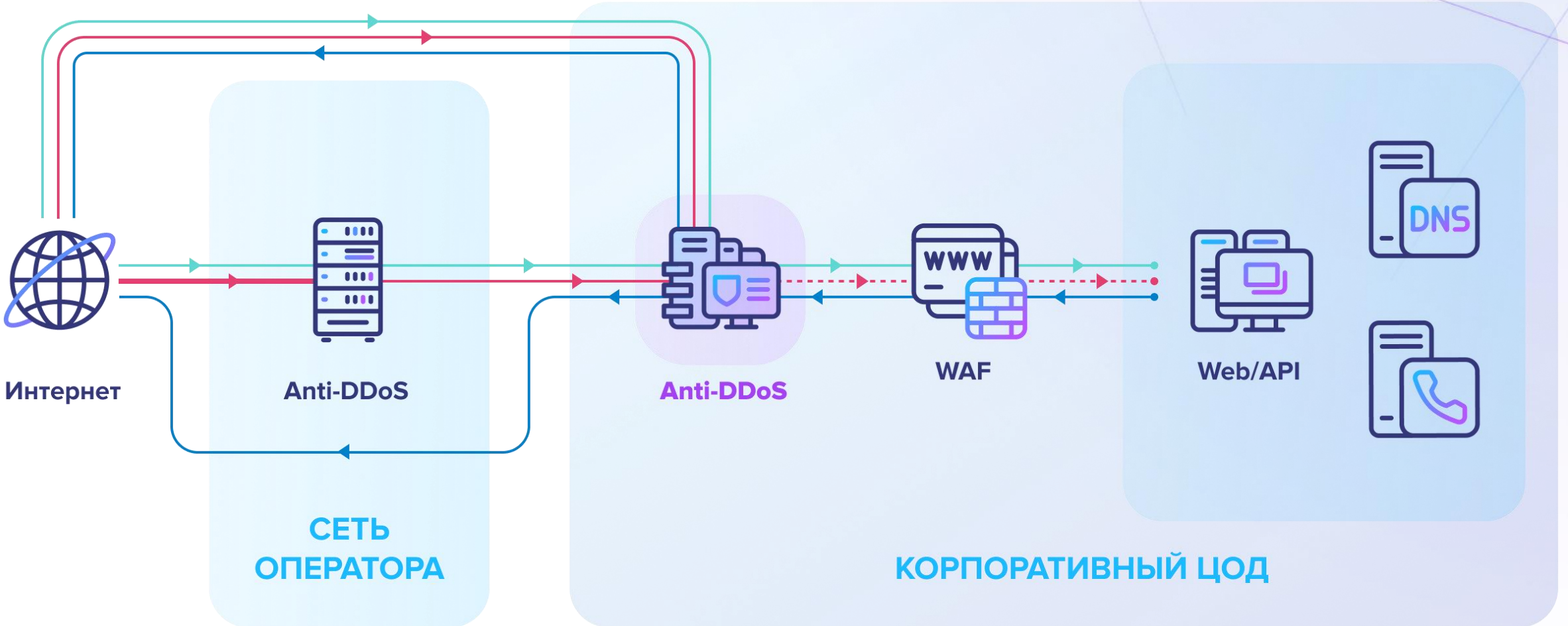
Двухуровневая защита...



...и её недостатки

«Третий элемент»

ГАРДА



Локальный Anti-DDoS должен уметь:

- ☑ Вскрывать и обрабатывать шифрованный трафик под нагрузкой.
- ☑ Работать как «умный провод» = не иметь собственных IP-адресов на интерфейсах обработки трафика.
- ☑ Защитить ВСЕ интернет-каналы компании.

Локальный Anti-DDoS должен уметь:

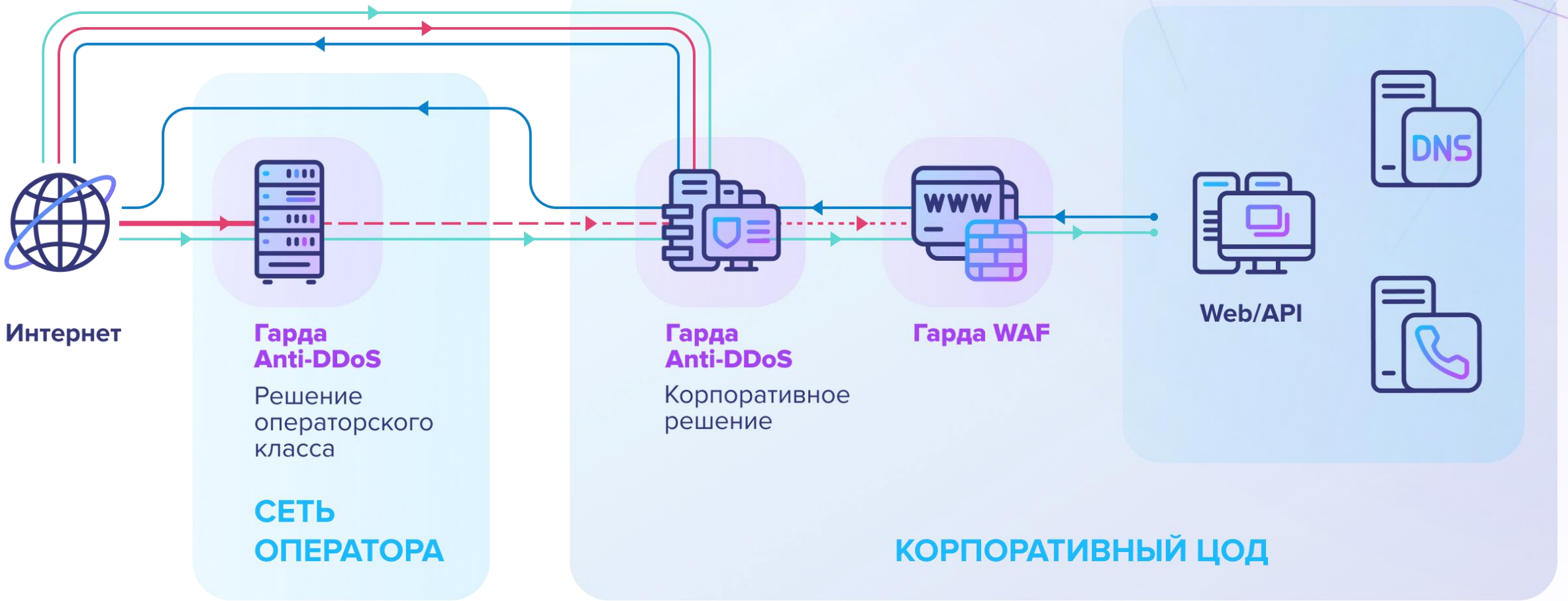
ГАРДА

- Фильтровать по «белым» и «черным» спискам IP-адресов с WAF.
- Работать на основе «прозрачных» настраиваемых алгоритмов.
- Анализировать логи защищаемого веб-сервера.

Локальный Anti-DDoS должен уметь:

- Использовать данные внешних репутационных баз для выявления и блокировки трафика из скомпрометированных источников.
- Сохранять информацию (метаданные) о проходящем трафике для ретроспективного анализа и расследования инцидентов.

Гарда Anti-DDoS



Гарда Anti-DDoS: противодействие

Атаки на каналы связи и уязвимости сетевых протоколов	
▪ ICMP Flood, ICMP Fragmentation Flood ▪ UDP Flood, Non-Spoofed UDP Flood, UDP Fragmentation Flood ▪ SYN Flood, SYN-ACK Flood, ACK Fragmentation Flood ▪ TCP Flood ▪ Ping Flood, Ping Of Death ▪ Атака поддельными TCP сессиями (Fake Session Attack, Multiple SYN-ACK Fake Session Attack) ▪ Атака поддельными TCP сессиями с несколькими ACK (Multiple ACK Fake Session Attack) ▪ RST/ FIN Flood ▪ VoIP Flood ▪ ICMP Redirect ▪ Sockstress ▪ IP spoofing	▪ TCP Hijacking ▪ Низкоуровневая атака (Naptha attacks) ▪ IP Null Attack, TCP Null Attack ▪ Атака широковещательными ICMP ECHO пакетами (Smurf Attack) ▪ Атака широковещательными UDP пакетами (Fraggle Attack) ▪ CharGEN Amplification ▪ ToS (Type of Service) Flood ▪ Атака фрагментированными пакетами со смещением (Teardrop Attack) ▪ Memcached Attack ▪ IoT Attack ▪ Сессионная атака. Атака медленными сессиями (Session attacks, SlowLoris) ▪ Неверные значения в заголовках пакетов, Land attack

Гарда Anti-DDoS: противодействие

Атаки с использованием протоколов уровня приложений	
▪ NTP Flood ▪ NTP Amplification ▪ HTTP Flood одиночными запросами (Single Request HTTP Flood, Multiple VERB Single Request) ▪ HTTP Flood одиночными сессиями (Single Session HTTP Flood, Excessive VERB Single Session) ▪ Атака фрагментированными HTTP пакетами (Fragmented HTTP Flood, HTTP Fragmentation, Nuke) ▪ HTTP GET Request ▪ HTTP POST Request ▪ Рекурсивный HTTP GET Flood случайными запросами (Random Recursive GET Flood) ▪ Рекурсивный HTTP GET Flood (Recursive HTTP GET Flood)	▪ DNS амплификация (DNS Amplification Attack), DNS Flood ▪ Rsyslog амплификация ▪ SSDP DDoS Attack ▪ SMTP Flood, SMTP Amplification ▪ SNMP Reflection ▪ SIP Register Flood, SIP Client Call Flood ▪ Атака модифицированными SIP-сообщениями (SIP Malformed Attack) ▪ Атака на приложение (Faulty Application Attack) ▪ Атаки на протоколы TLS/SSL, MitM, подмена сертификатов ▪ HTTPS GET Request ▪ HTTPS GET Flood ▪ HTTPS POST Request ▪ HTTPS POST Flood ▪ HTTPS Flood

Гарда Anti-DDoS

- Вскрытие шифрованного трафика до **25 000 TPS на 20 Гбит/с.**

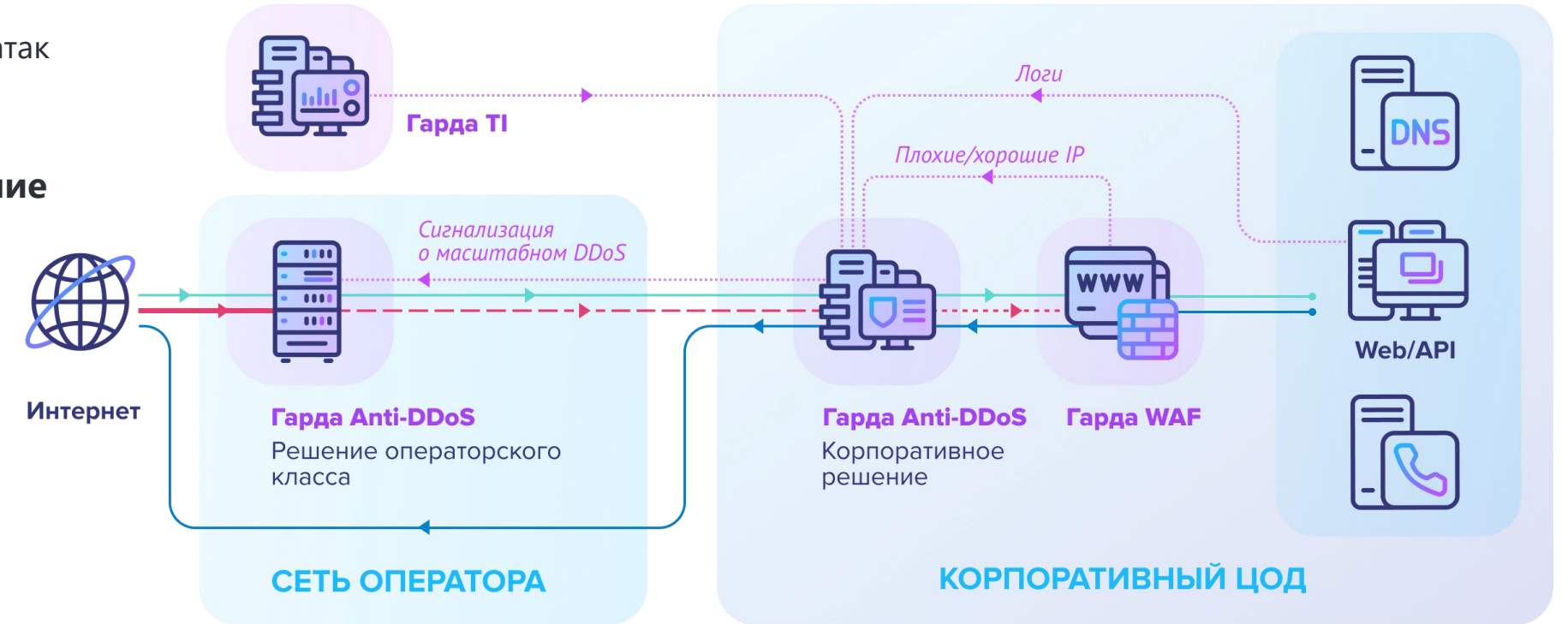
- **Автоматизация типовых действий и реакций на атаки:**
  - шаблоны противодействия под каждый тип защищаемых ресурсов;
  - автоматическое профилирование проходящего трафика.

- **Существенное снижение нагрузки на службу эксплуатации заказчика.**

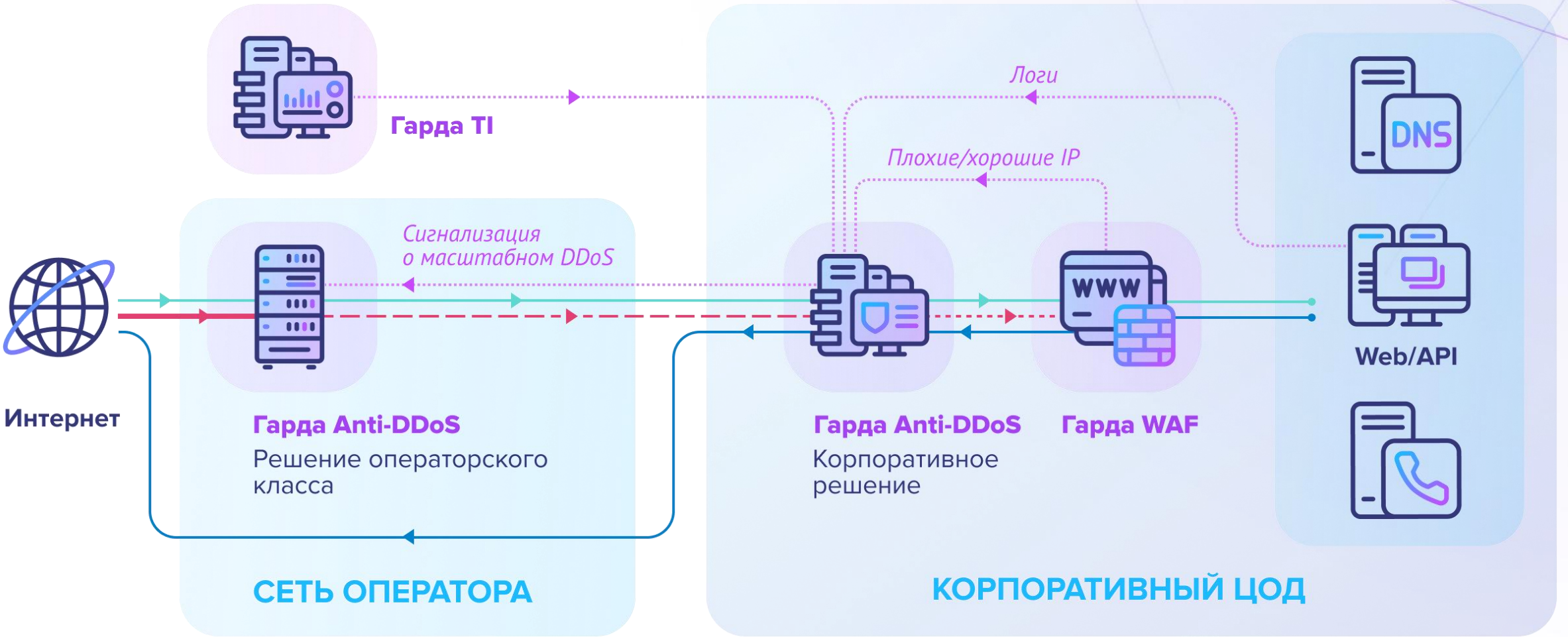
Эшелонированная защита

Продукты «Гарды» используют для построения эшелонированной защиты:

- **«Гарда Anti-DDoS» операторского класса**
  для защиты от объемных атак
- **«Гарда Anti-DDoS» корпоративное решение**
  для локальной защиты
- **«Гарда WAF»**
  для целевой защиты веб-ресурсов
- **«Гарда TI»**
  сервис «фидов» киберугроз



Эшелонированная защита



ГАРДА

Гарда Anti-DDoS
Преимущества

Экспертиза и соответствие требованиям

17+ лет опыта разработки, поддержки и развития Anti-DDoS решения

В промышленной эксплуатации у требовательных федеральных заказчиков

Сертификат ФСТЭК на Требования доверия (4), Требования к СЗИ от DDoS(4)

Отечественное ПО в Реестре Минцифры

Удобство эксплуатации

ГАРДА

Автоматизация работы и понятные алгоритмы мер противодействия

Подходящие конфигурации для небольших и географически распределённых сетей

Возможности масштабирования перекрывают любые запросы заказчиков

Работает на стандартных серверах x86-64

Функциональность и интеграция

Фильтрация атак в шифрованном трафике (HTTPS), в т.ч. с возможностью вскрытия

Возможность сбора и хранения метаданных о трафике для ретроспективного анализа атак и аномалий

Собственный протокол облачной сигнализации для эшелониро-ванного подавления крупных атак

Интеграция с внешними репутационными базами и системами сетевой безопасности, включая «Гарда TI» и «Гарда WAF»

GARDA

Подписывайтесь
на телеграм-канал **garda.ai**

Спасибо за внимание!

garda.ai
info@garda.ai