Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

# Level 3® DDoS и Web Security

АНДРЕЙ ЗЕЛЕНОВ
Сентябрь 2016

# Level 3 Communications – коротко о компании:

Level (3) COMMUNICATIONS
Connecting and Protecting the Networked World℠

| Level 3 Communications | |
|---|---|
| Over $8B Pro Forma LTM Revenue* |
| Approx. 12,500 Employees |
| Hallo Hello 你好 Olá Bonjour ¡Hola — Connecting 60+ Countries and Counting |
| 200,000+ Route Miles of Fiber Globally |
| Approx. 350 Multi-tenant Datacenters |
| Over 43Tbps of Global IP Capacity |
| More than 12B+ Minutes Per Month in VoIP Traffic |

| Level 3 Customers | |
|---|---|
| 8 of the Top 10 U.S. Based Banks |
| 8 of the Top 10 Internet Service Providers |
| 8 of the Top 10 Global Pharmaceutical Companies |
| 8 of the Top 10 Cable MSOs |
| 8 of the Top 10 World's Most Valuable Brands |
| 4 of the "Big 6" Movie Studios |

# Подходы к защите от DDOS, применяемые компаниями

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

I. **Собственное программно-аппаратное решение защиты от DDOS**

Преимущества: Контроль, доступ к экспертизе вендора

Ограничения: Цена/стоимость владения: CAPEX + OPEX + **Capacity**, Экспертиза, Масштаб

II. **Облачные решения (1) - Специализированные компании («pure play»)**

Преимущества: OPEX, Экспертиза, Независимость от операторов

Ограничения: Масштаб; Конечная емкость аплинков; потребуется наладить взаимодействие IT/Network/Security внутри компании и с поставщиком решения

III. **Облачные решения (2) - Специализированные сервисы крупных операторов**

Преимущества: OPEX, Экспертиза, Независимы от операторов, Устойчивость при крупных атаках + возможность блокировать ботнеты в местах их «обитания», Превентивная диагностика за счёт глобального мониторинга

Ограничения: потребуется наладить взаимодействие IT/Network/Security внутри компании и с поставщиком решения

Возможны варианты: собственная система + поддержка оператора (Network protection), собственная система + облачная платформа …

# Роль провайдера в организации защиты

***The Expanding Role of Service Providers in DDoS Mitigation (Frost & Sullivan, 2015)***

- Service provider has far more network visibility and data to collect and analyze for threats compared to even a large enterprise network. This visibility gives service providers a great advantage in the effort to identify attacks.
- Service providers can block threats upstream at the network edge closest to the malicious hosts.
- By combining these two advantages, service providers may be able to block attacks by identifying the activities that precede a DDoS attack.
- The advancement of service provider DDoS mitigation services wouldn't necessarily compete with enterprise DDoS mitigation solutions, as many organizations will continue to require an on-site solution that can complete their DDoS protection strategies. However, hybrid and cloud models are currently the most effective mitigation strategies for defending against the largest DDoS attacks.

# Роль провайдера в организации защиты

***The Expanding Role of Service Providers in DDoS Mitigation (Frost & Sullivan, 2015)***

- Поставщик услуг имеет гораздо большую видимость сети и данных для сбора и анализа угроз по сравнению с даже большой корпоративной сетью. Эта видимость дает поставщикам услуг большое преимущество в целях выявления атак.
- Поставщики услуг могут блокировать угрозы на границе своей сети, ближайшей к источнику атаки.
- Комбинируя эти два преимущества, поставщики услуг могут блокировать атаки путем выявления событий, которые предшествуют DDoS-атаке.
- Преимущества поставщика услуг совсем не обязательно будут конкурировать с корпоративными решениями по защите от DDoS, так как многие организации будут по-прежнему использовать решения «на месте» чтобы дополнить свою стратегию защиты от DDoS. Тем не менее, использование гибридной и облачной модели в настоящее время является наиболее эффективной стратегией для защиты от самых крупных DDoS-атак.

# Что мы видим и делаем

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

We **monitor**
~1.3 billion
Security events per day

We **respond** to and
mitigate ~40
DDoS attacks a day

We **identify** and **remove**
at least one C2
network a month

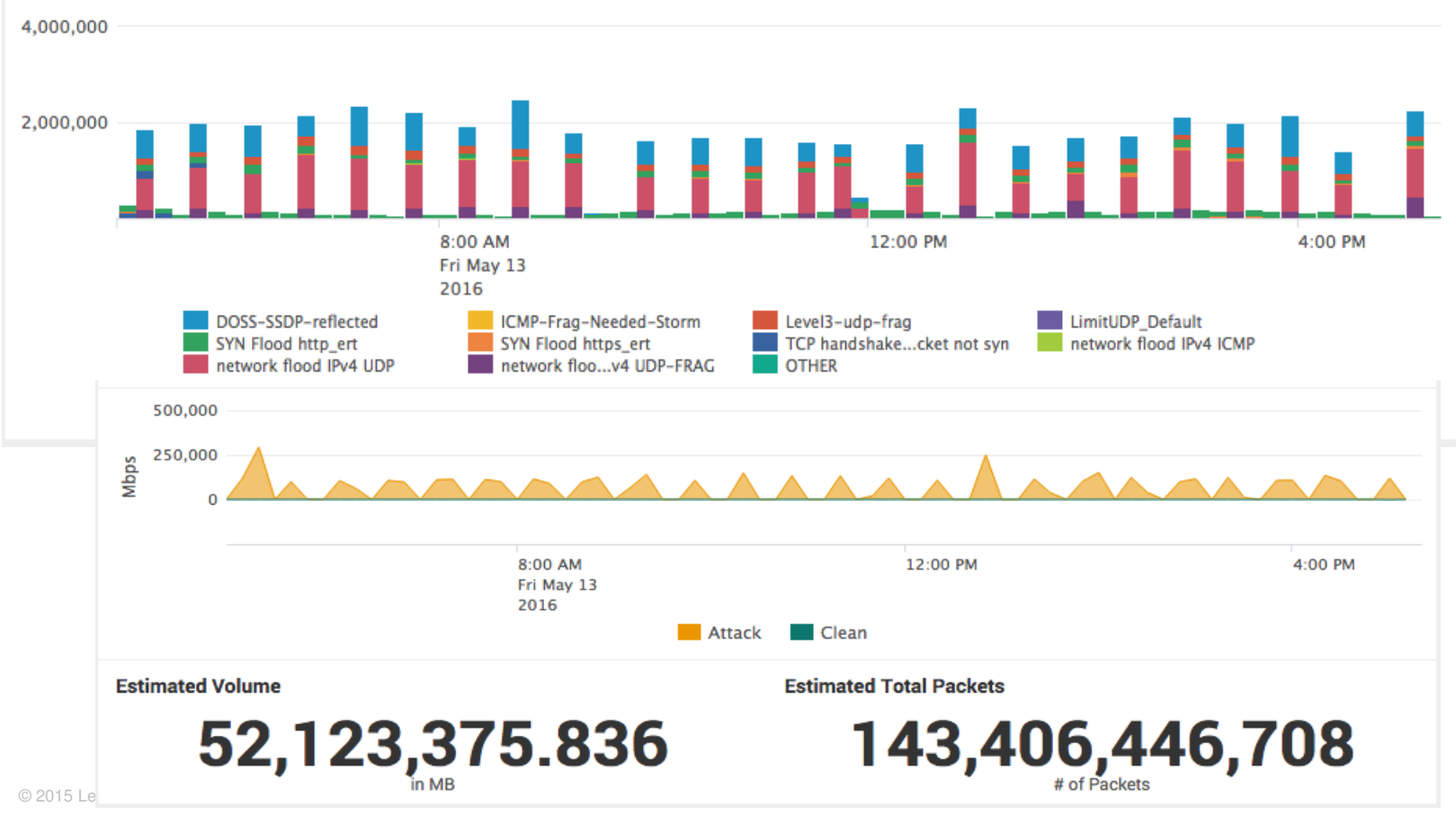
We **monitor** over
48 billion
NetFlow sessions per day

We **collect**
~87 TB of data
per day

We perform
daily audits,
protect and monitor
**all** our products & systems

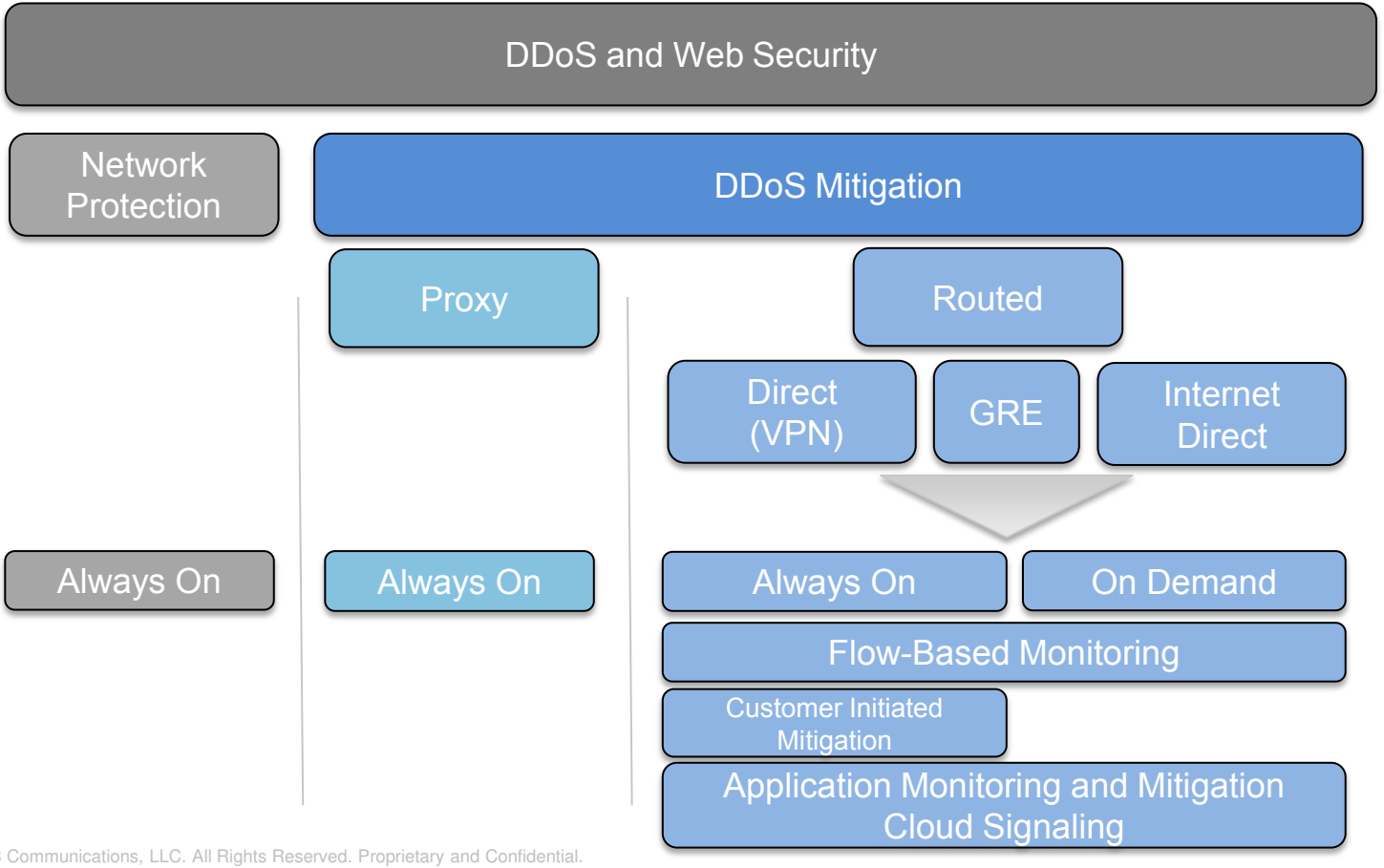
# Отбитая масштабная атака ~250 Gbps

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠



# Взаимодополняющие уровни защиты

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

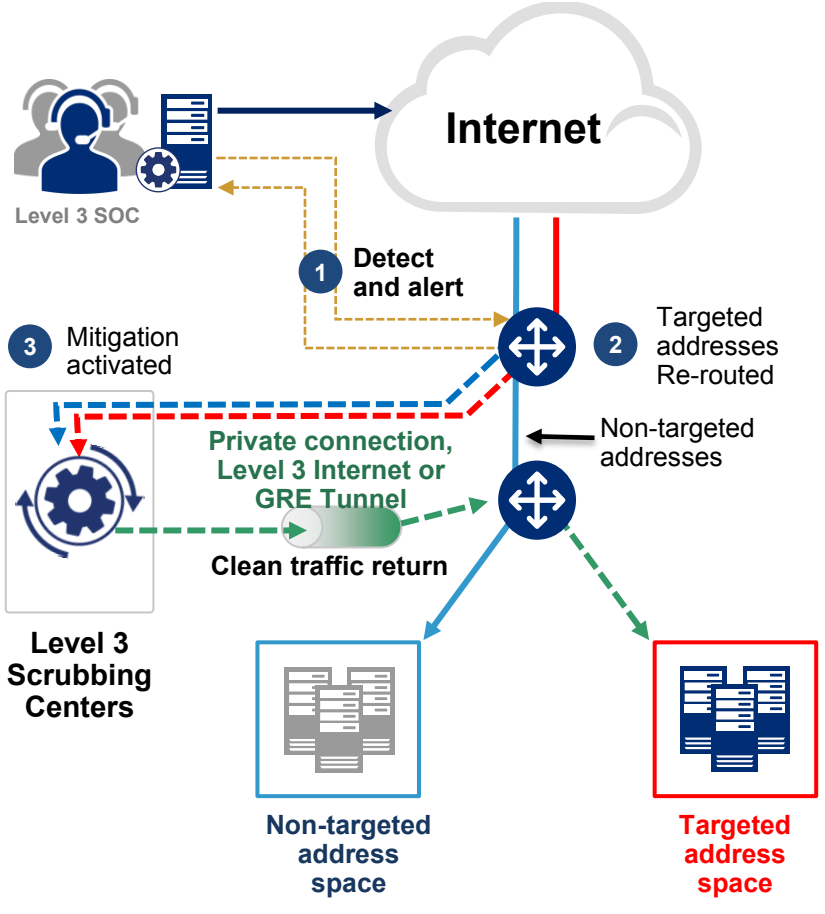


# Как Это Работает

1. **Detection:** Attack identified by Customer or Level 3 SOC (On Demand)
2. **Re-Route:** BGP used to route traffic through Scrubbing Centers (On Demand)
3. **Mitigation:** Targeted address traffic diverted and scrubbed
4. Command & Control server take-downs performed as appropriate

## Service Highlights

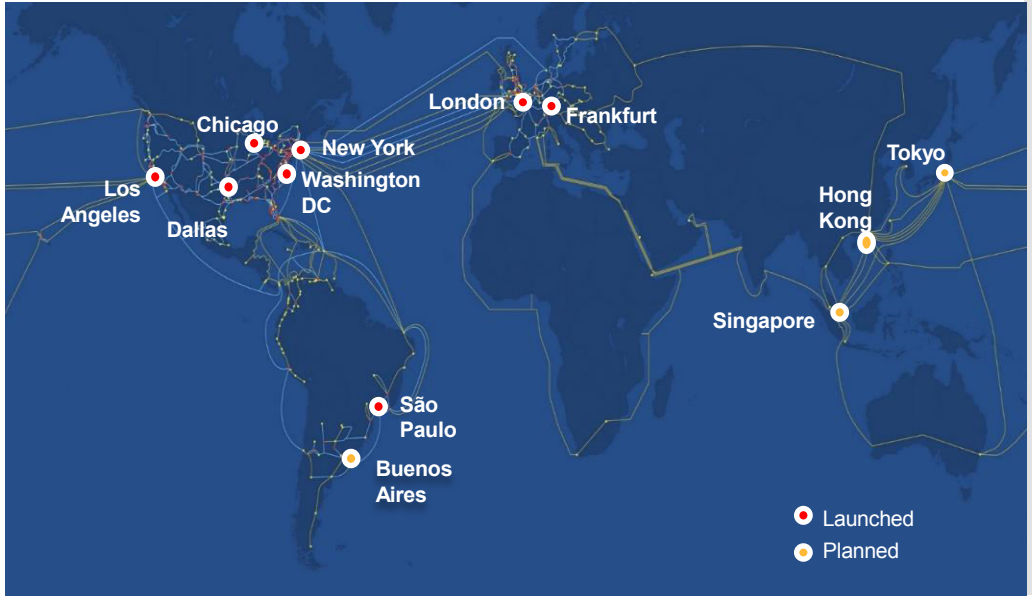
- Network-based, unlimited mitigation
- Always-On or On-Demand options
- Route determined by BGP configuration
- Asymmetric traffic flow
- Private connection for forwarding clean traffic
- Volumetric and application layer attack mitigation (Layers 3-7)
- Optional Flow-Based Monitoring (proactive monitoring and alerting)



# Level 3® DDoS Mitigation Service

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

## Глобальная система защиты на основе собственной сети



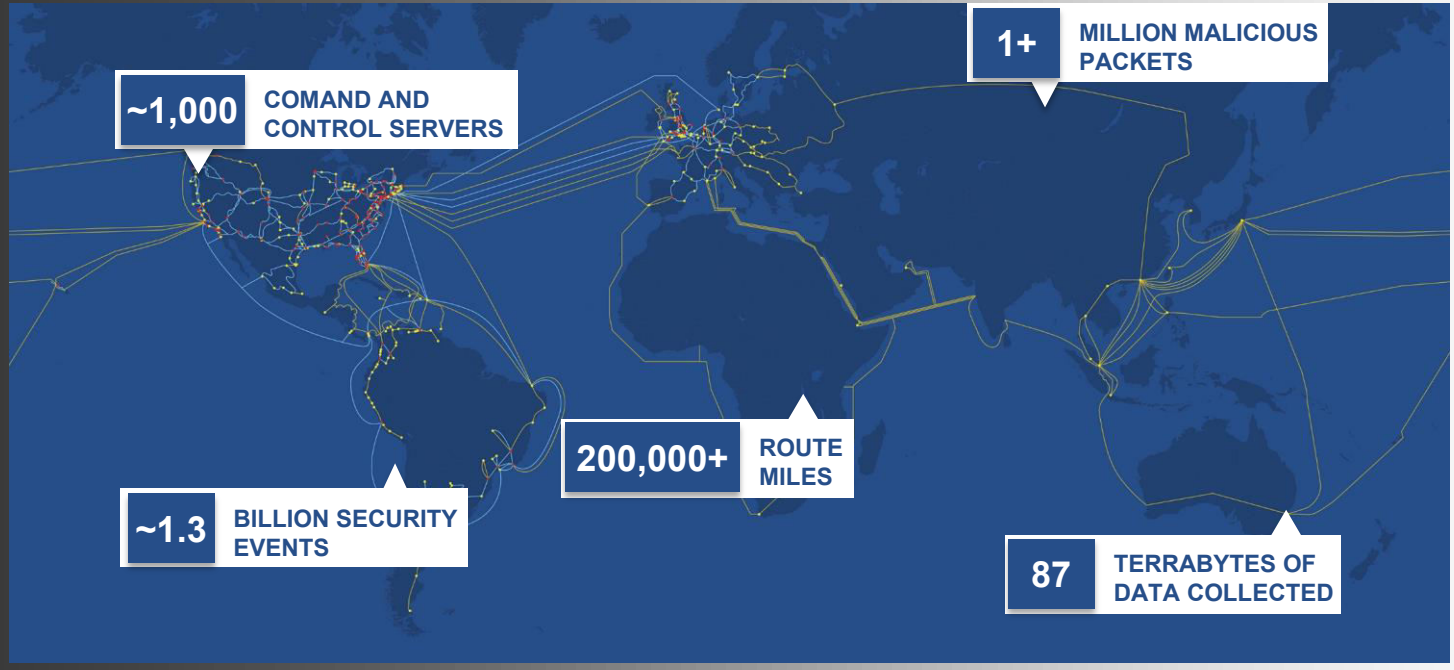

- Network-based security
- 4.5 Tbps of ingest capacity
- Carrier agnostic
- Regionally distributed scrubbing centers
- Network-based controls
- Extensive peering
- Backed by threat Intelligence generated by Level 3 Threat Research Labs
- Supported 24x7 by global Security Operations Centers

# Security Is Our Core

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

***EVERY DAY, AROUND THE CLOCK , WE TRACK, MONITOR AND MANAGE:***

24/7 365



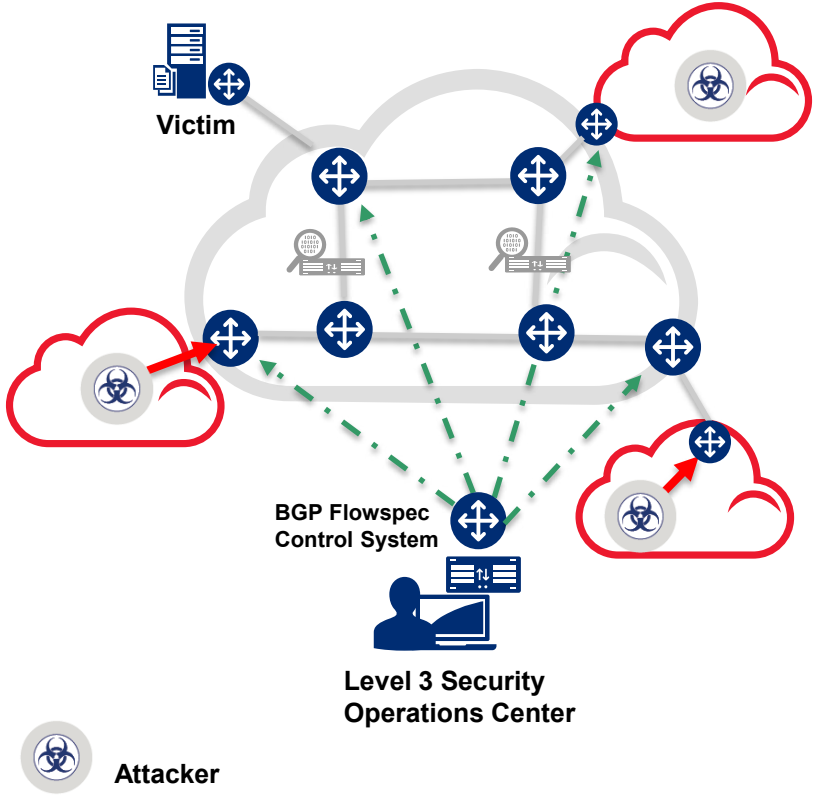
# Расширенные возможности Level 3

## Использование BGP Flowspec для быстрой реакции

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

### Expected to be the largest scale deployments in the Industry

- BGP Flowspec based announcements allow for an automated ACL rules delivery to Level 3 Flowspec capable routers.
- Highly scalable solution, available globally, managed by the Level 3 Security Operations Center
- Facilitates emergency mitigation
- **Key Benefits:**
  - Rapid deployment of ACLs globally
  - Provides an additional layer of mitigation against large scale volumetric attacks on network layers 3 and 4



# Заключение

- Количество, размер и сложность DDoS атак растёт
- DDoS – по природе глобальная проблема, требующая глобальных решений
- Для эффективной защиты нужен комплексный подход
- Выбор способа защиты от DDoS индивидуален и зависит от профиля потенциальной жертвы: собственно цель, размер и тип бизнеса, масштаб угроз
- Сотрудничество с операторами связи – неотъемлемый элемент политики защиты от DDoS
- Технологические методы защиты – важнейший элемент политики, но не панацея.


Level (3) COMMUNICATIONS

Connecting and Protecting the Networked World℠

# Спасибо!

Level 3 COMMUNICATIONS

Connecting and Protecting the Networked World℠

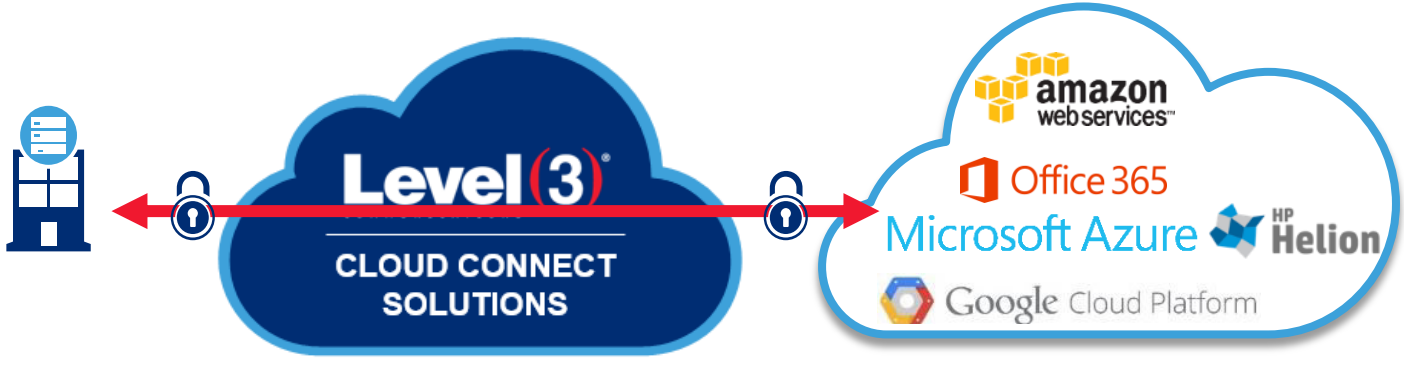
***Мы пойдем другим путем ;-)***

# LEVEL 3® CLOUD CONNECT SOLUTIONS

## PRIVATE, SECURE CONNECTIVITY TO THE CLOUD

Level 3 COMMUNICATIONS
Connecting and Protecting the Networked World℠

**Level 3 Cloud Connect Solutions** offer a private network ecosystem that can connect your enterprise with leading cloud and data center providers around the world. They can provide improved application performance as well as security and flexibility, which allow you to realize all the benefits of the cloud without compromising productivity or revenue.




**SCALE NETWORK AND BANDWIDTH ON DEMAND**

**PRIVATE CONNECTIVITY TO THE CLOUD**

**FLEXIBLE ETHERNET AND IP VPN CONNECTIVITY OPTIONS**

**CONNECT TO CSP LOCATIONS GLOBALLY**