JETSECURITY
CONFERENCE 2018

Защищая самое важное: данные и приложения

Александр Крошкин
alexander.kroshkin@imperva.com

28 мая, 2018
Radisson Resort, Zavidovo

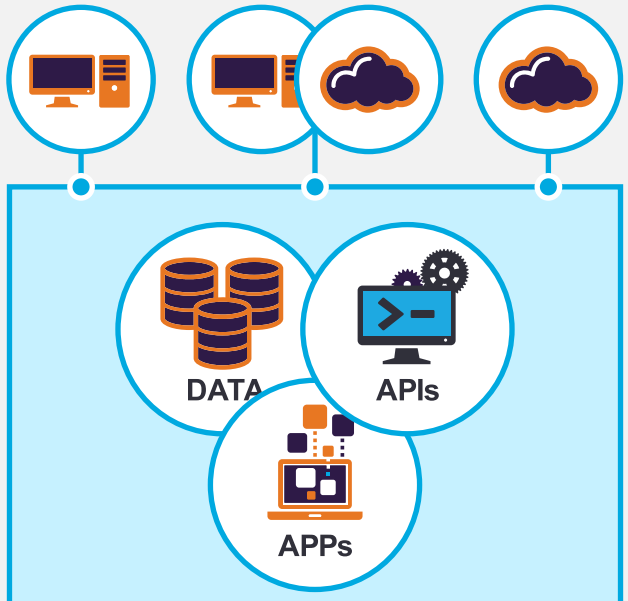
Outside the Organization

- Partners
- Customers
- Contractors
- Bad bots
- Hackers

SECURE APP DELIVERY

- CDN
- Load balancing
- WAF
- DDoS
- Bot Protections

ON-PREM HYBRID CLOUD



DATA SECURITY & COMPLIANCE

- Visibility
- Policies
- Reporting
- Monitoring
- Blocking
- Masking

SIEM

Inside the Organization

- Trusted
- Privileged
- Malicious
- Careless
- Compromised

Product Lines

Application Security

DDoS Protection
(+CDN +WAF)

Web App Firewall

IMPERVA INCAPSULA

IMPERVA SECURESPHERE

IMPERVA THREATRADAR

Data Security

Data Masking

Database & File
Activity Monitoring

CAMOUFLAGE

IMPERVA SECURESPHERE

IMPERVA COUNTERBREACH

IMPERVA®

Universal User Tracking case study

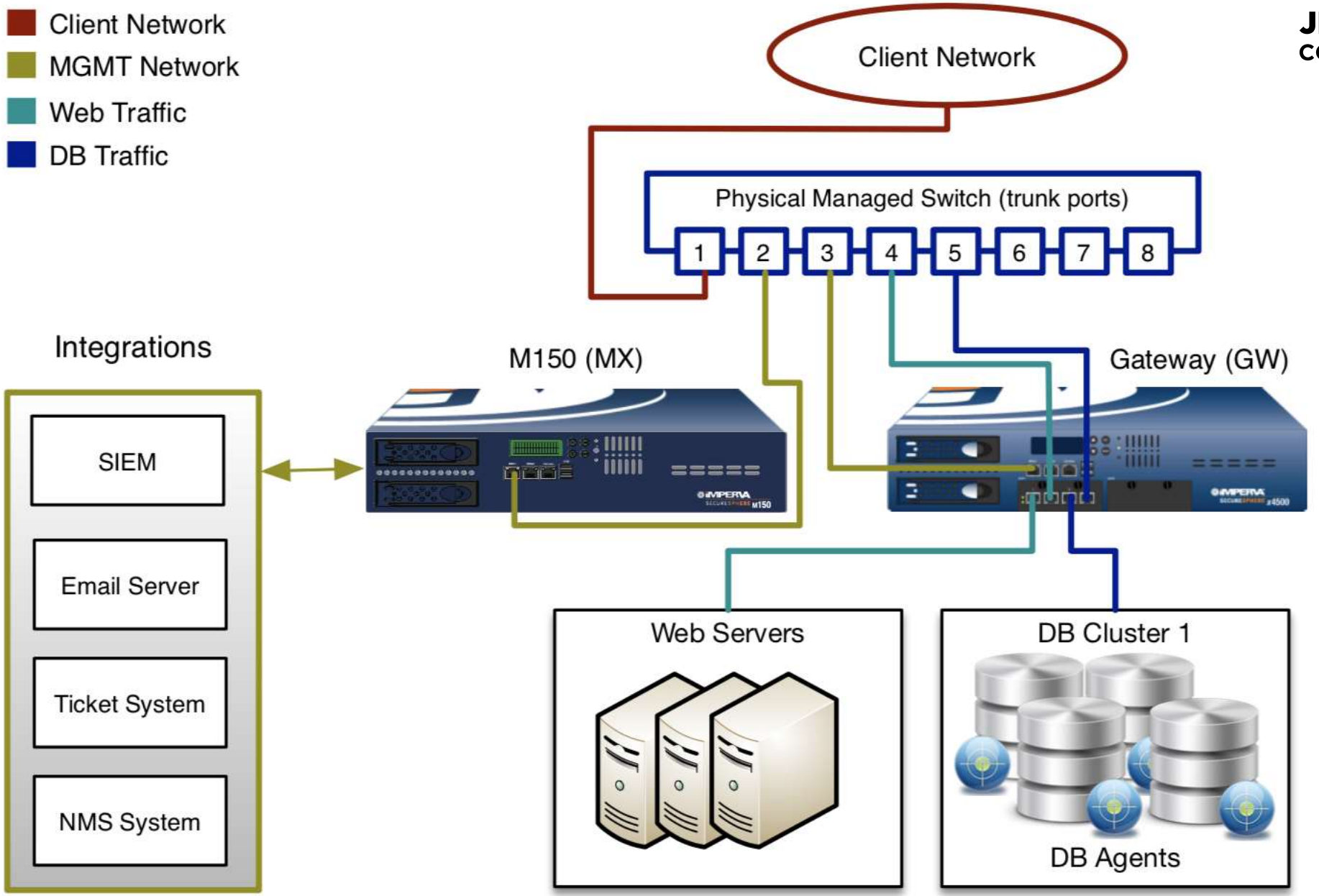
IMPERVA SECURESPHERE

JETSECURITY CONFERENCE 2018

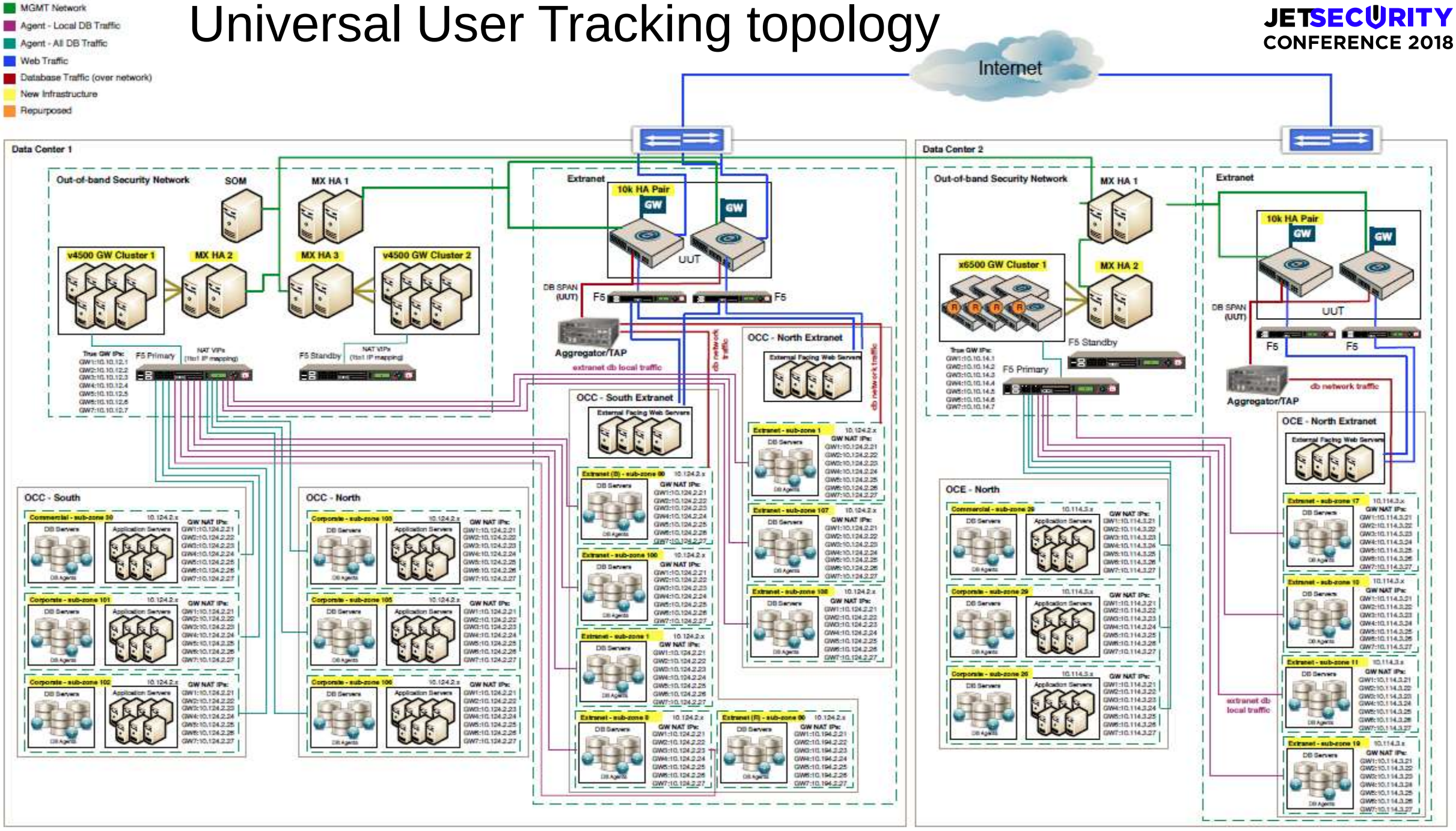
- **Complex Data Environment:**
  - Apps: Internal business critical, Customer facing and APIs, Transactional
  - DBs: RDMS, Big Data, Mainframe
  - Scale: 1,500+ DB servers
  - Web to DB user correlation: ie. “Bob Smith” not “App Account” generic pooled connection

- **Solution:**
  - SecureSphere WAF + DAM/DBF
  - Mix of both inline & out-of-band
  - Mix of both physical (2 & 10 Gbps) & virtual appliances
  - Automation – 150 DB agents deployed per weekend for ~10 weeks
    - Combination of *SCCM, Blade Logic, Chef, & Puppet* to push agents + configurations

Universal User Tracking case study reference architecture



Universal User Tracking topology



Product Lines

Application Security

DDoS Protection
(+CDN +WAF)

Web App Firewall

IMPERVA INCAPSULA

IMPERVA SECURESPHERE

IMPERVA THREATRADAR

Data Security

Data Masking

Database & File
Activity Monitoring

CAMOUFLAGE

IMPERVA SECURESPHERE

IMPERVA COUNTERBREACH

From zero to a breach detection dashboard in 6 WEEKS

Before	After
2% of DB traffic monitored	**50%** of DB traffic monitored
0.25 FTE	**0.25** FTE
1,000 alerts per day	**15-30** alerts per day
1% of alerts investigated	**100%** of alerts investigated
0 significant incidents discovered	**2** significant incidents discovered

RESULTS

25x more DB traffic monitored

Equivalent FTE

1000x reduction in rate of alerts

100x increase in alerts investigated

IMPERVA

IMPROVED EFFECTIVENESS OF DATA SECURITY WITHOUT INCREASED LABOR COSTS

Before	After
7.2 Billion transactions in 60 days	**732** incidents
10,000 Splunk alerts per week	**12** incidents per day
2 FTE	**2** FTE
10% of alerts investigated	**100%** of alerts investigated
0 significant incidents discovered	**6** significant incidents discovered

RESULTS

Manageable # of alerts

Equivalent FTE

All incidents investigated

Machine learning
no tuning

914k DB records accessed by 1 person

Early Breach Detection Requires Additional Intelligence

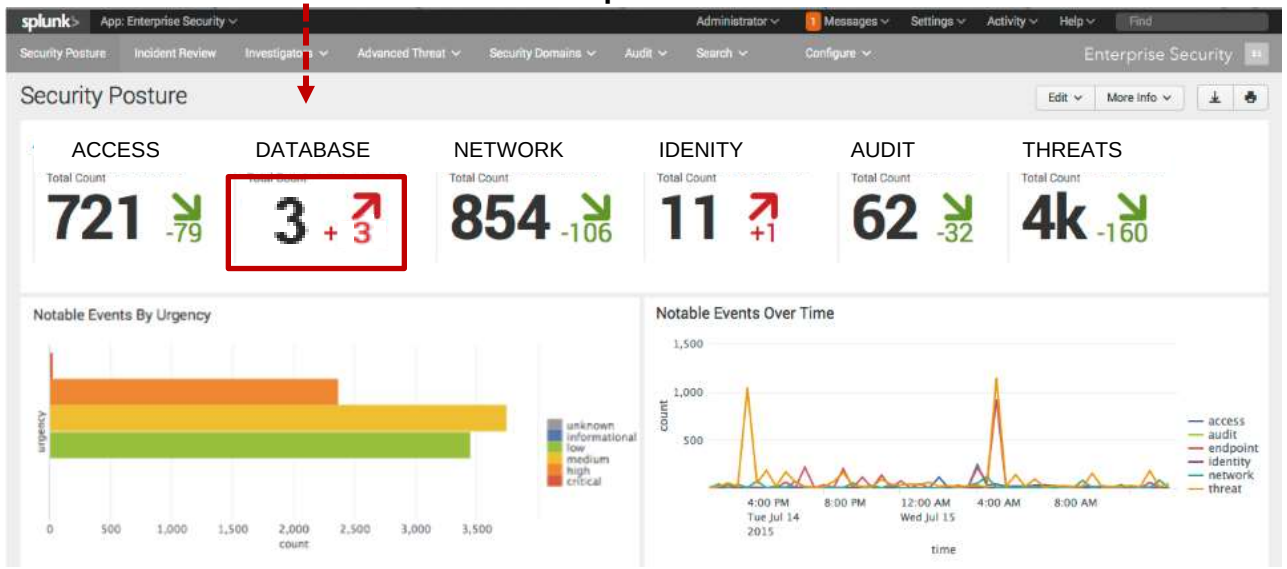
Databases

IMPERVA COUNTERBREACH

Behavior Analytics

Machine Learning

Enterprise SIEM



Trusted Globally in Banking and Financial Services

JETSECURITY
CONFERENCE 2018

Спасибо за внимание!

БОЛЬШЕ ЧЕМ БЕЗОПАСНОСТЬ