

“What went wrong when
your bank was hacked?”

Nezar Nassr

July 2020

► EastNets Investigations and conclusions on
recent fraud cases

 **EastNets®**
financial integrity. delivered.



COMPLIANCE
SOLUTIONS

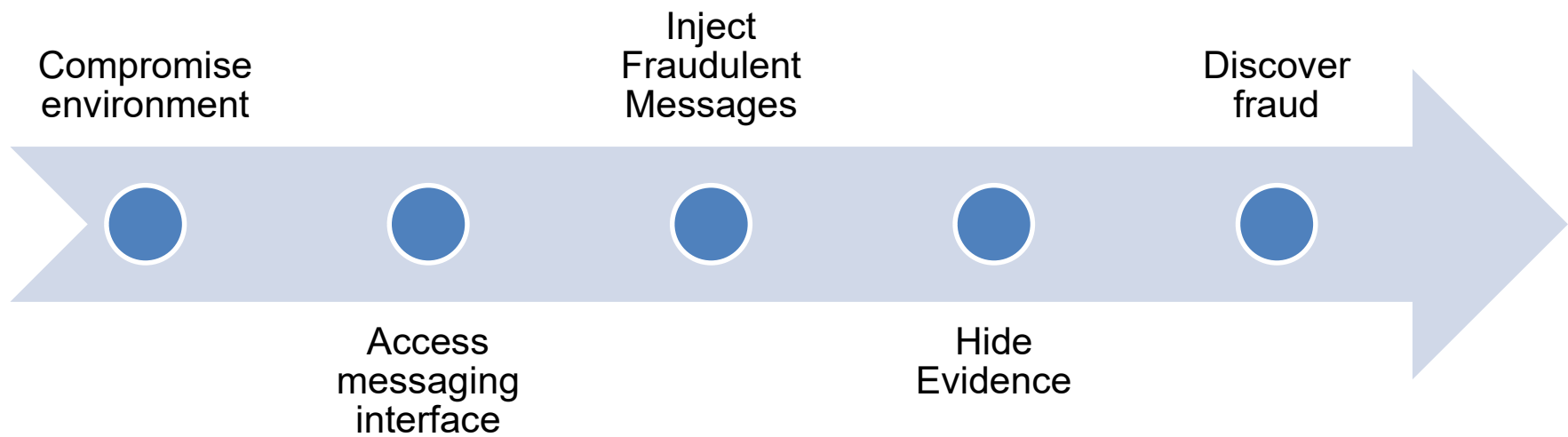


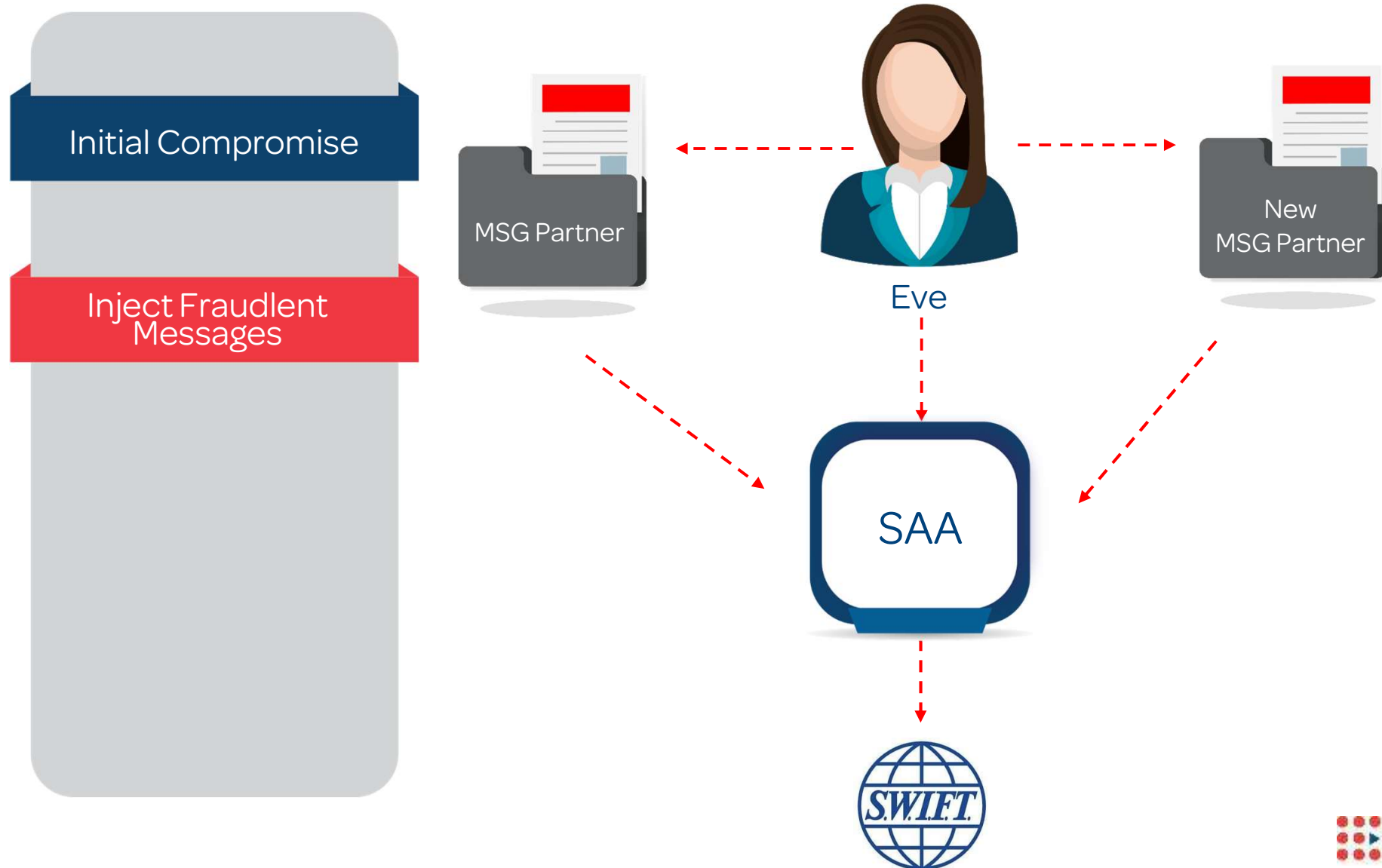
PAYMENT
SOLUTIONS



CLOUD
SOLUTIONS

Modus operandi of a cyber attack





Initial Compromise

Inject Fraudulent
Messages

Sender: BICBICBIC
Receiver: CIBCIBCI

:20:REF123

:32A:180226GBP525,00

:50K:/BE290500000000

John Smith
Brussels
Belgium

:57A:ADCB AEAA

:59:/US12345
New York
USA
.....

Currencies

- USD
- EUR

Beneficiary
Banks

- Dubai
- Hong Kong
- Turkey
- China
-

Amounts

- >= 500K

Formatting

- Well
formatted

Timing

- Evening
- Morning

Number of
Messages

- Less than –
15
Messages



Initial Compromise

Inject Fraudulent
Messages

Hide Evidences

Fraud Detection

How?

When reconciling Nostro-Vostro accounts,
from MT940, MT950



How do they react?

Message cancellation

But...

instant payments are the norm now



Initial Compromise

Inject Fraudulent Messages

Hide Evidences

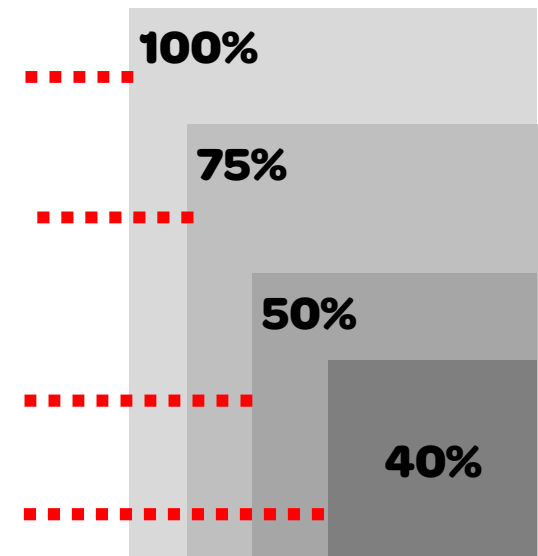
Fraud Detection

100% within 24 hours.

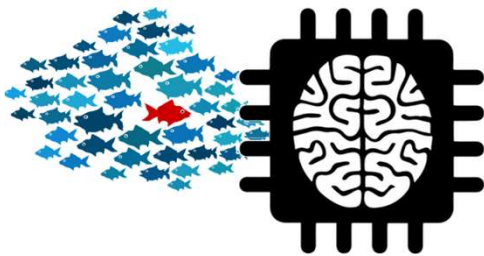
within 6 hours

are credited within 30 minutes

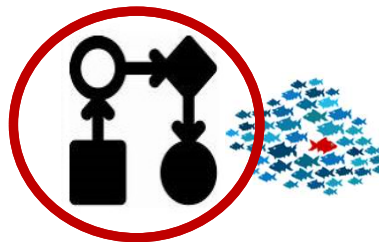
are credited to end beneficiaries
within 5 minutes



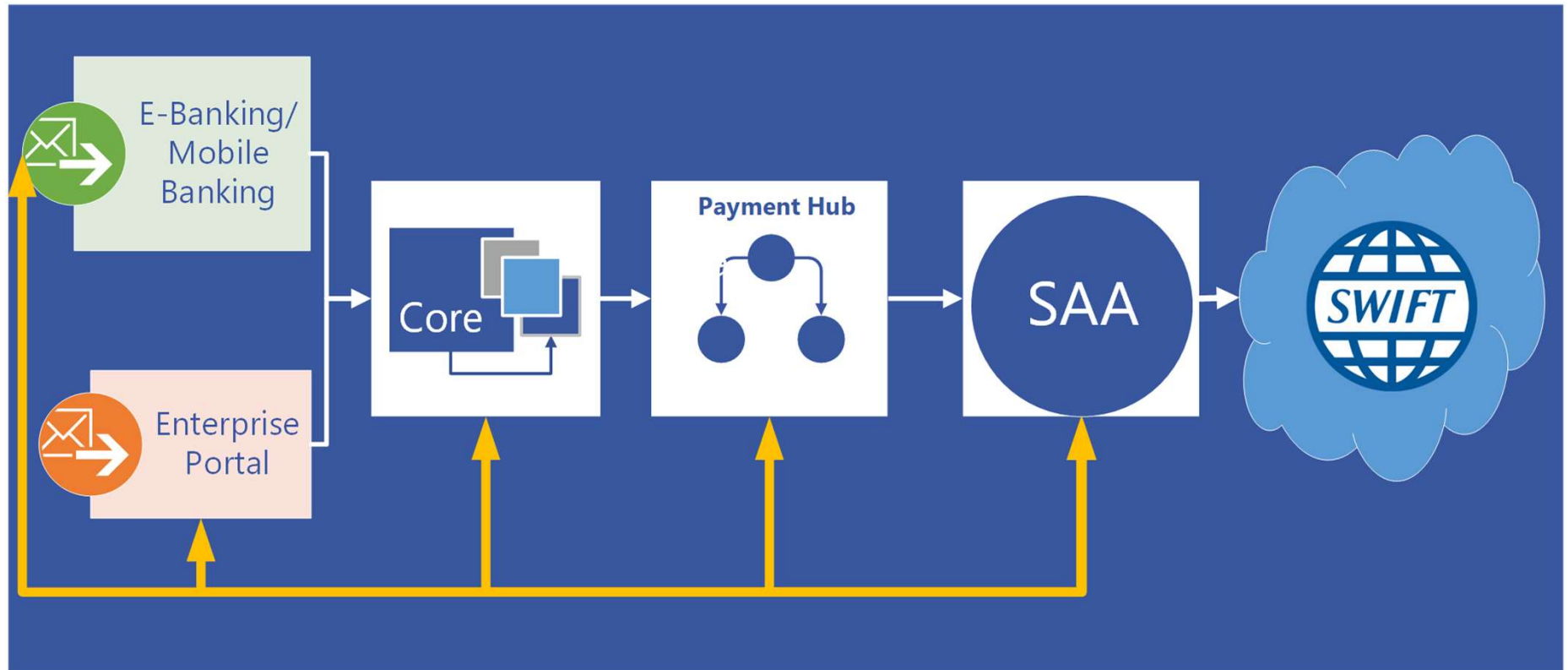
- **Real-Time Message Analysis:**



- **Events**

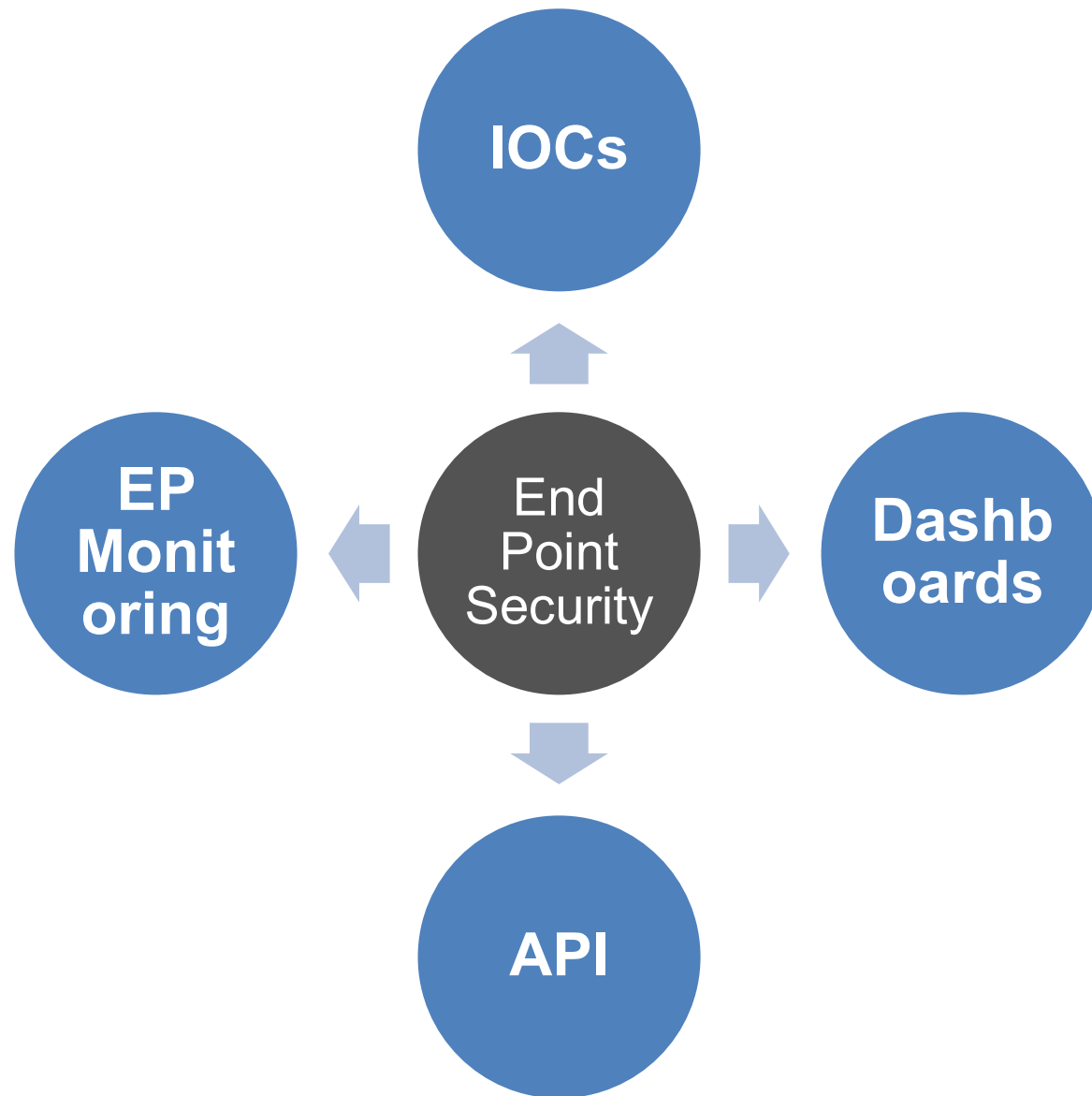


Message Authenticity/Payments Reconciliation



- Orchestral Scenario:
 - Risk level associated with each member scenario
 - A global threshold is associated with the orchestral scenario
 - Some member scenarios can be mandatory (AND operator)





If you are hacked, can your fraud detection get disabled?

Yes

?

How

ADK: uses queues
How: change routing
schema

Y-Copy
How: disable Y-
Copy



Mitigation Levels

Real-time
Interception
Before
Network


Real-Time
In Network

Sent MSGs
Immediately
Post Network

Notifications
Within
Minutes Post
Network



Going beyond existing fraud detection mechanisms



Verify message
authenticity using gpi
tracker



Stop and recall



- **Go beyond the scope of SWIFT CSP**
- **Develop a resilient cyber incident response plan**
- **Deploy a real-time Payment Fraud solutions**
- **In-network message authenticity controls**

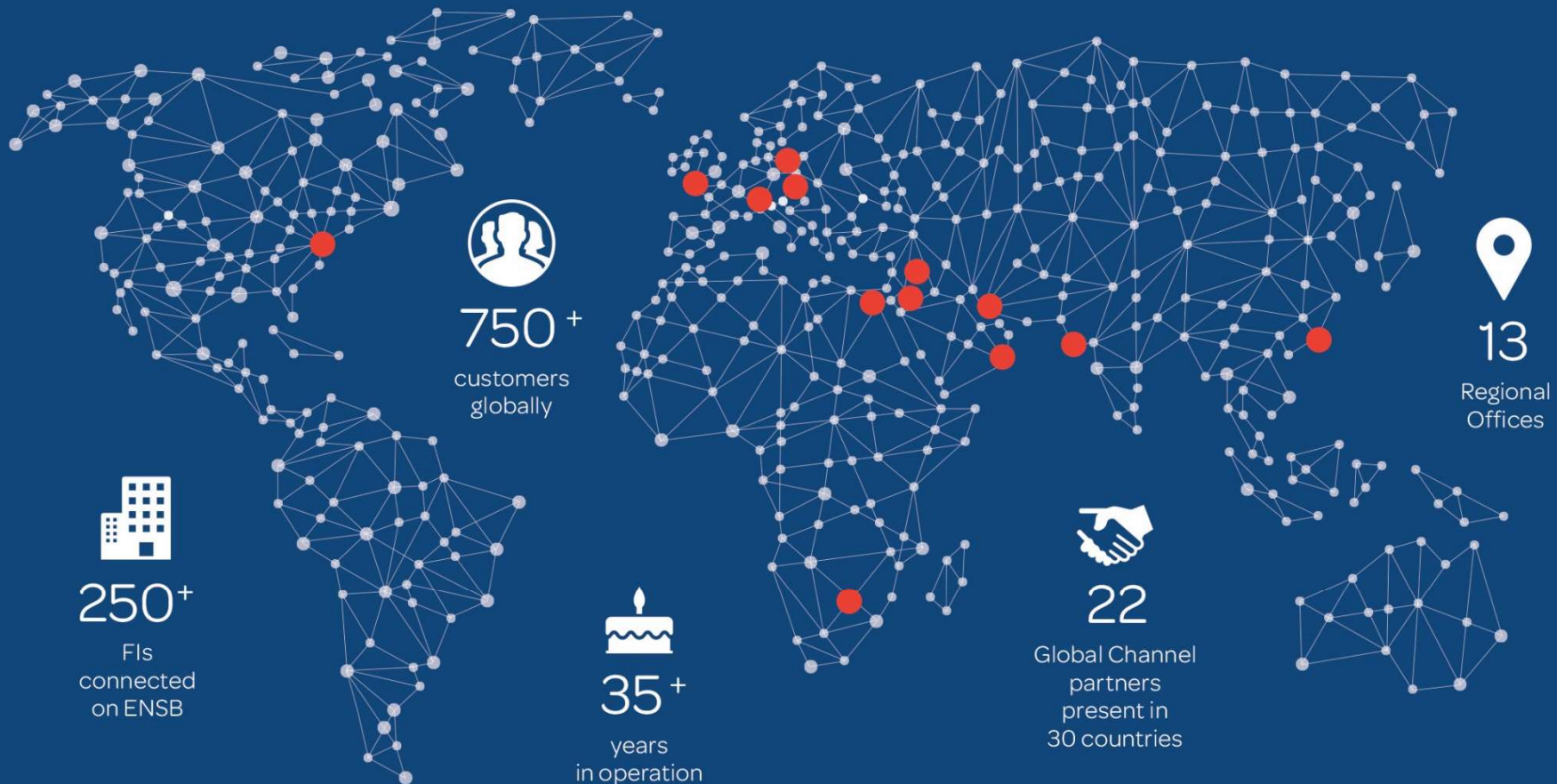


What do you think ? Any questions ?



EastNets®

financial integrity. delivered.



Waterloo • Luxembourg • London • Paris • New York • Sao Paulo • Dubai • Amman • Cairo • Bahrain • Doha • Karachi • Hong Kong