Secure Network Communication

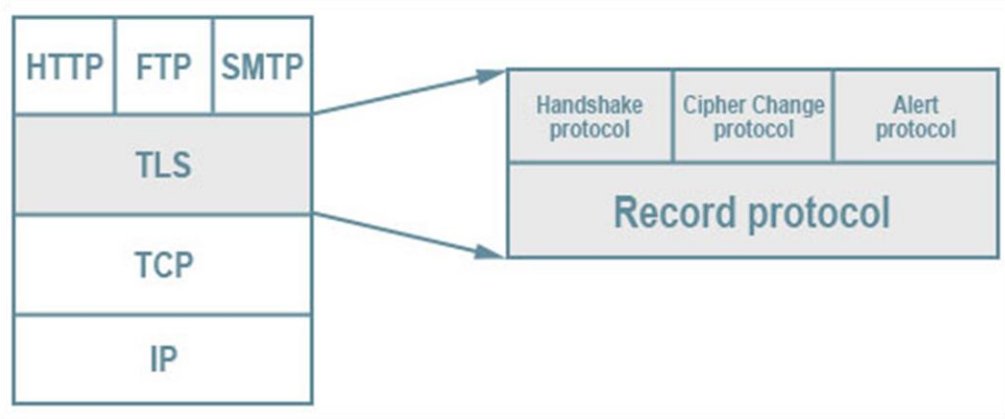
6th June 2018

Jason Huggins
Director, Global Delivery

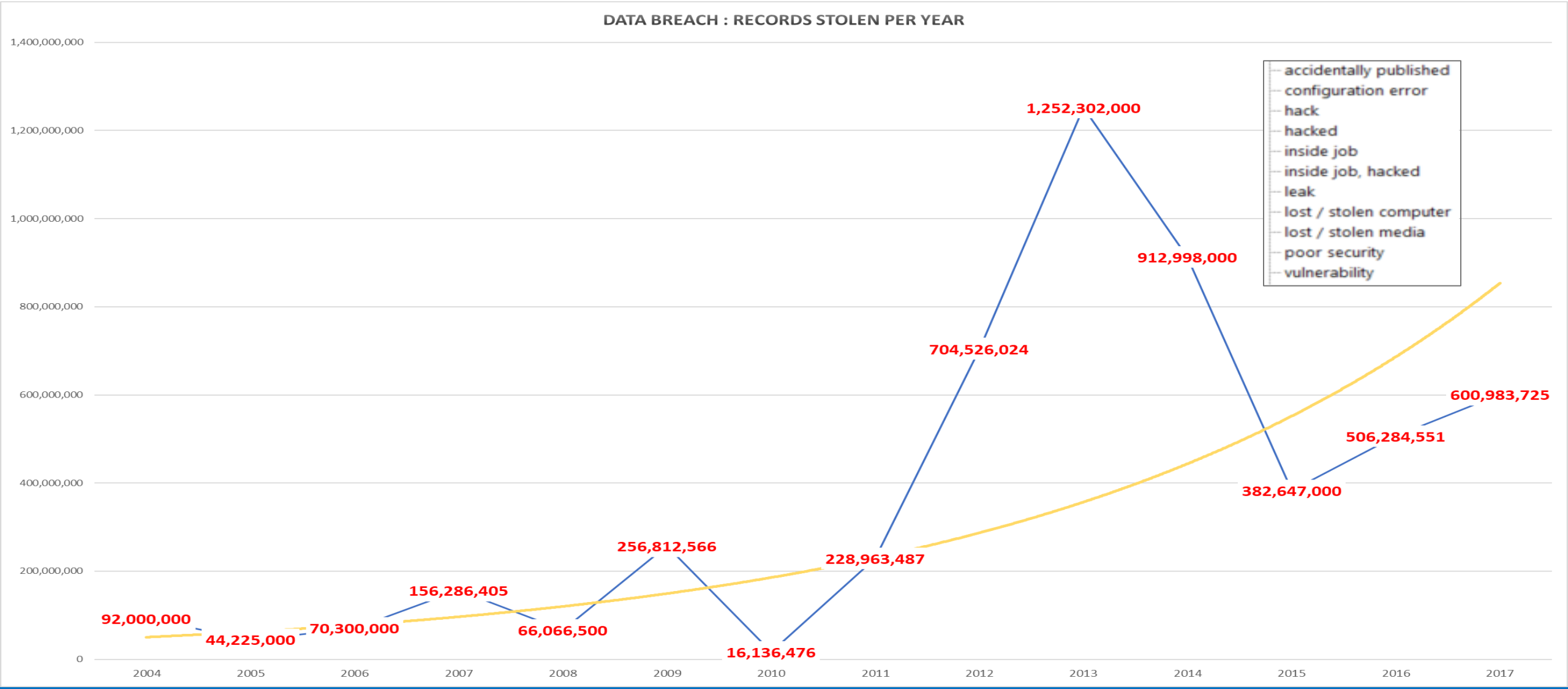
Agenda

UNIFACE 10
Enterprise Edition

- The need for data security
- The TLS solution
- Considerations

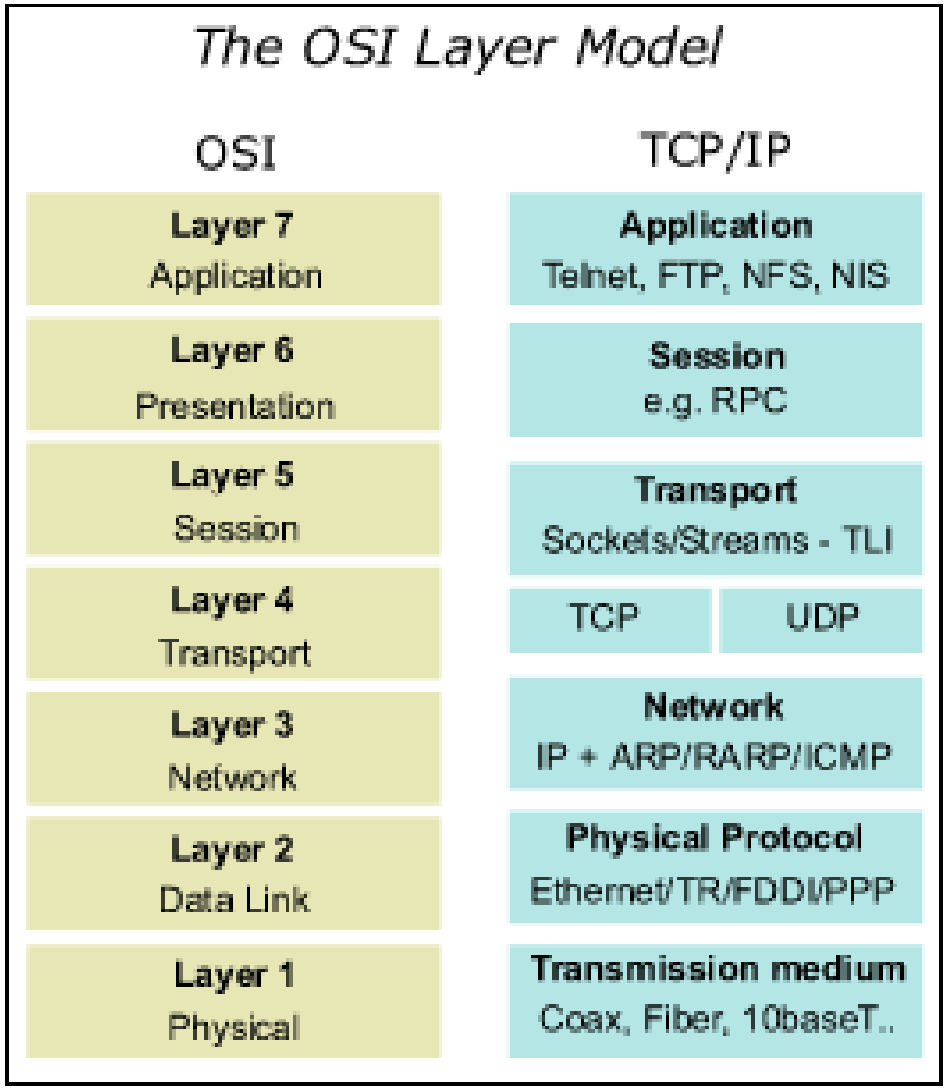


Global data breach statistics



UNIFACE

A key contributor is the network



Cryptography is important for ~~Uniface~~ all apps!

- Threats to network traffic are increasing

>80%

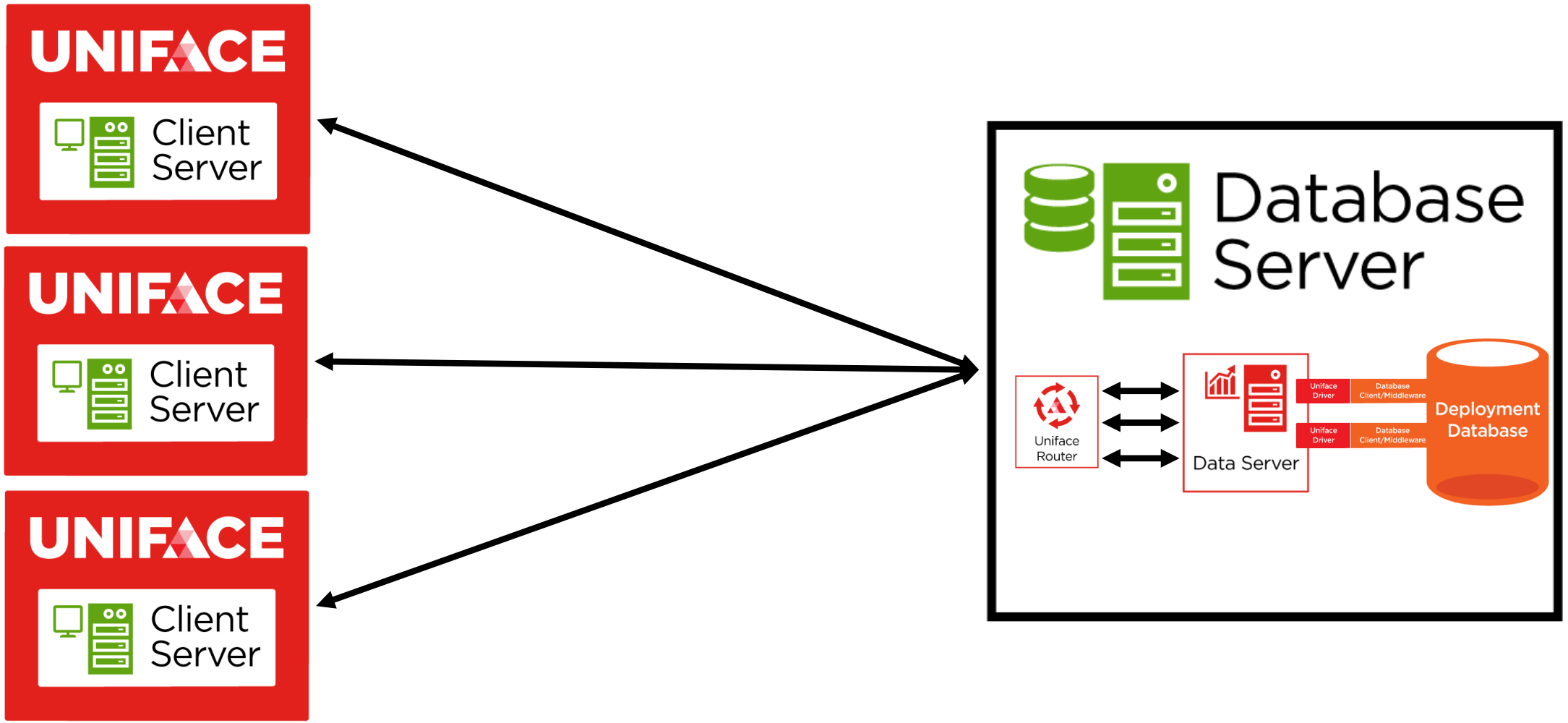
of enterprise traffic will be encrypted through 2019[1]

[1] [Source: Gartner Predicts 2017: 'Network and Gateway Security]

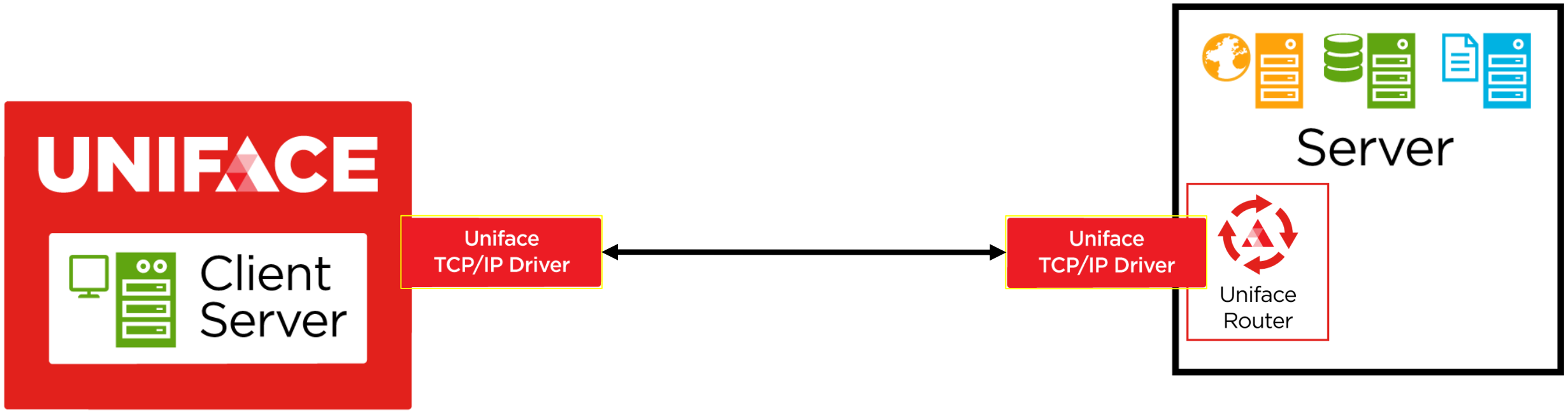
Consequences

- Average cost of a data breach ~$4M
- Identity theft in US cost ~$16Bn in 2014 alone
- GDPR fines
  - Up to €10 million or 2% of annual global turnover
  - Up to €20 million or 4% of annual global turnover

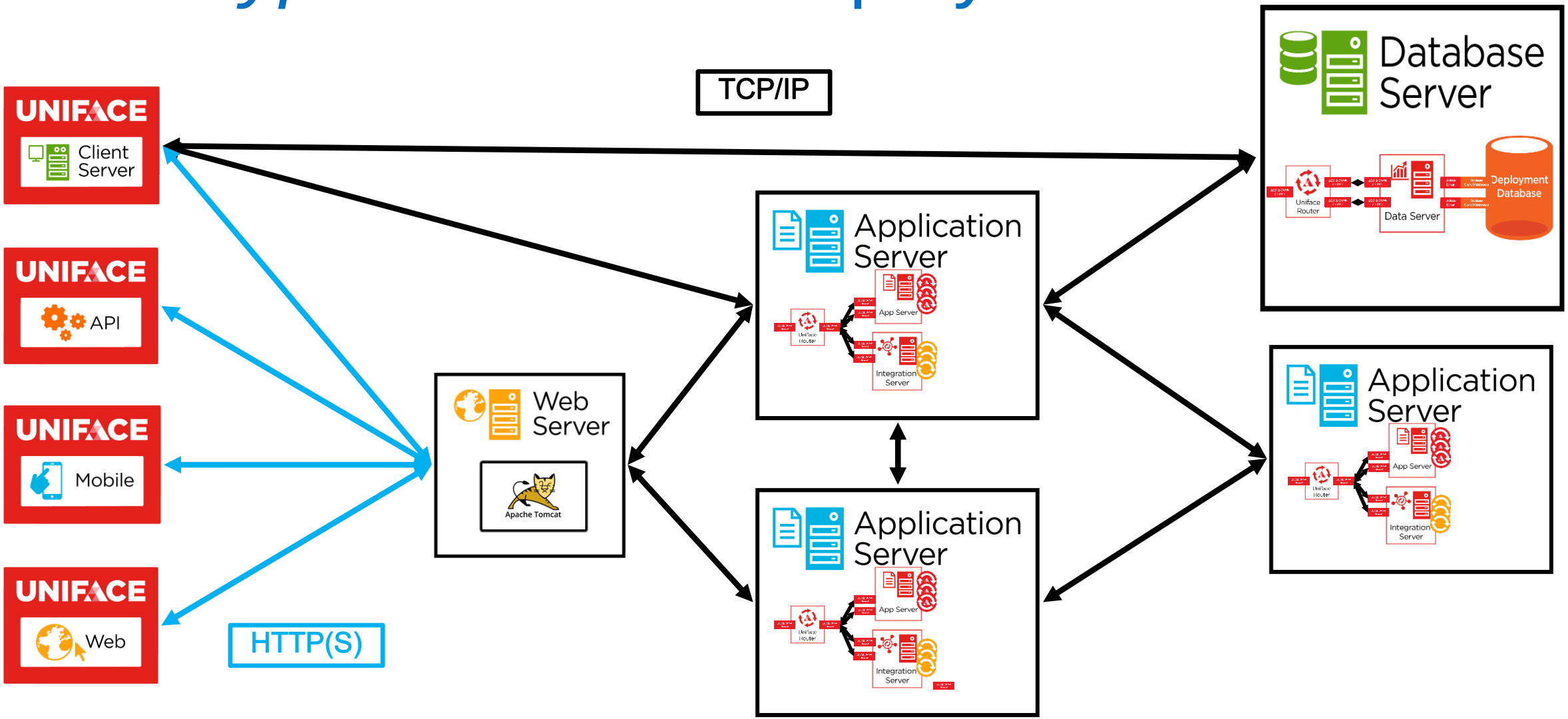
A simple Uniface deployment



We use TCP/IP for our communication protocol



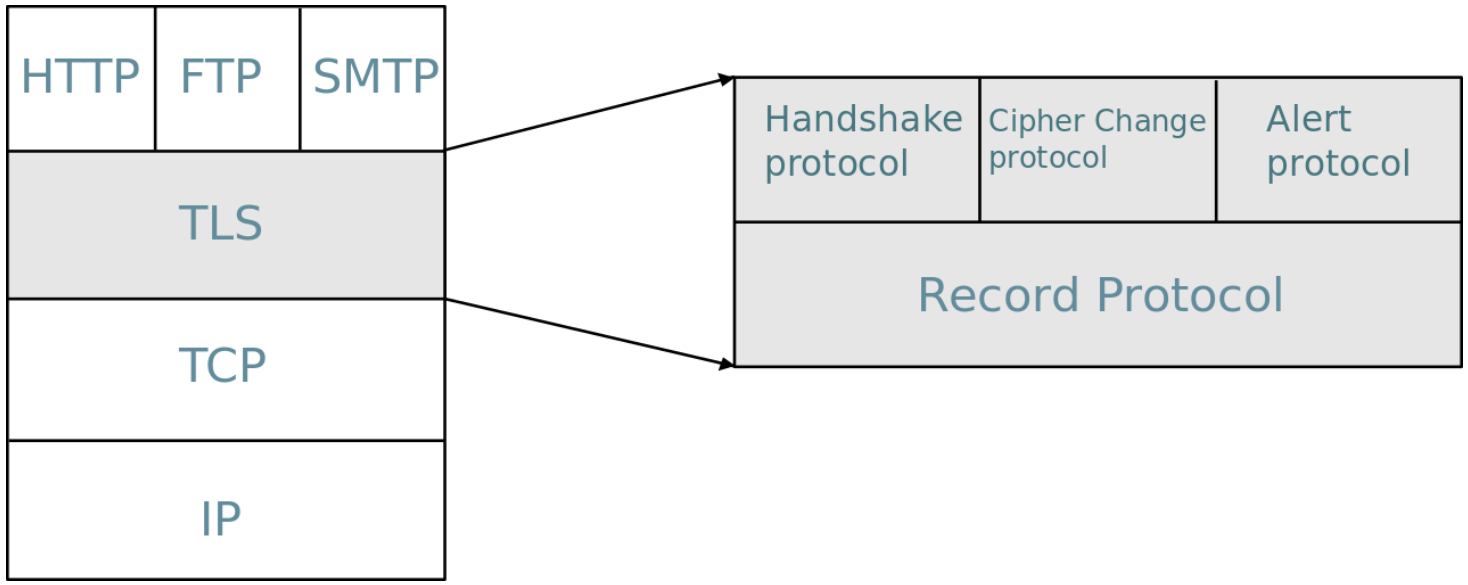
A more *typical* Uniface Deployment



So, what is the solution?

Transport Layer Security

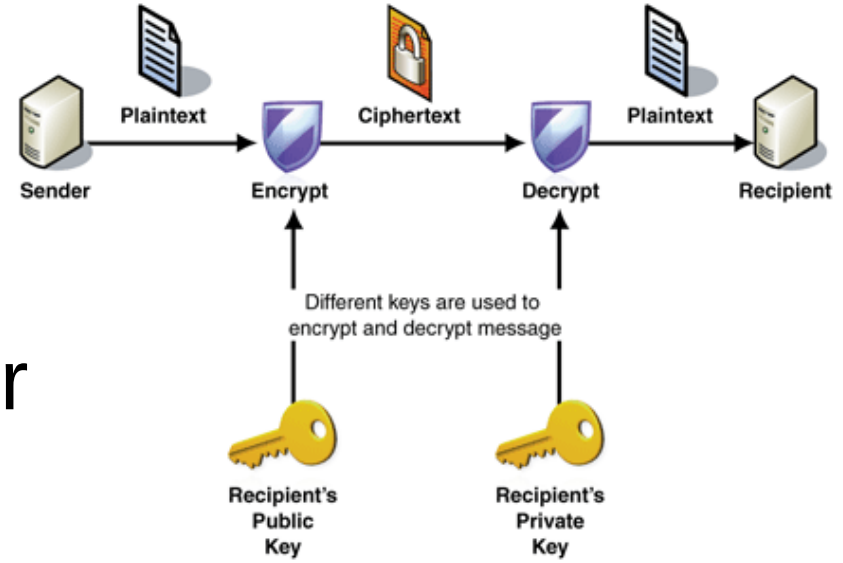
- Cryptographic protocols secure communications
- Successor to Secure Sockets Layer (SSL)
  - More secure
  - Greater efficiency



What we have done

Implemented a TLS driver

- Added a cryptography layer to our network stack
- Utilised OpenSSL
- Pre-shared key and Asymmetric certificate/key pair verification
- Peer name verification
- Both shared and exclusive servers
- IPV6
- Refactored & improved the TCP/IP driver
- **Simple Configuration**



OpenSSL

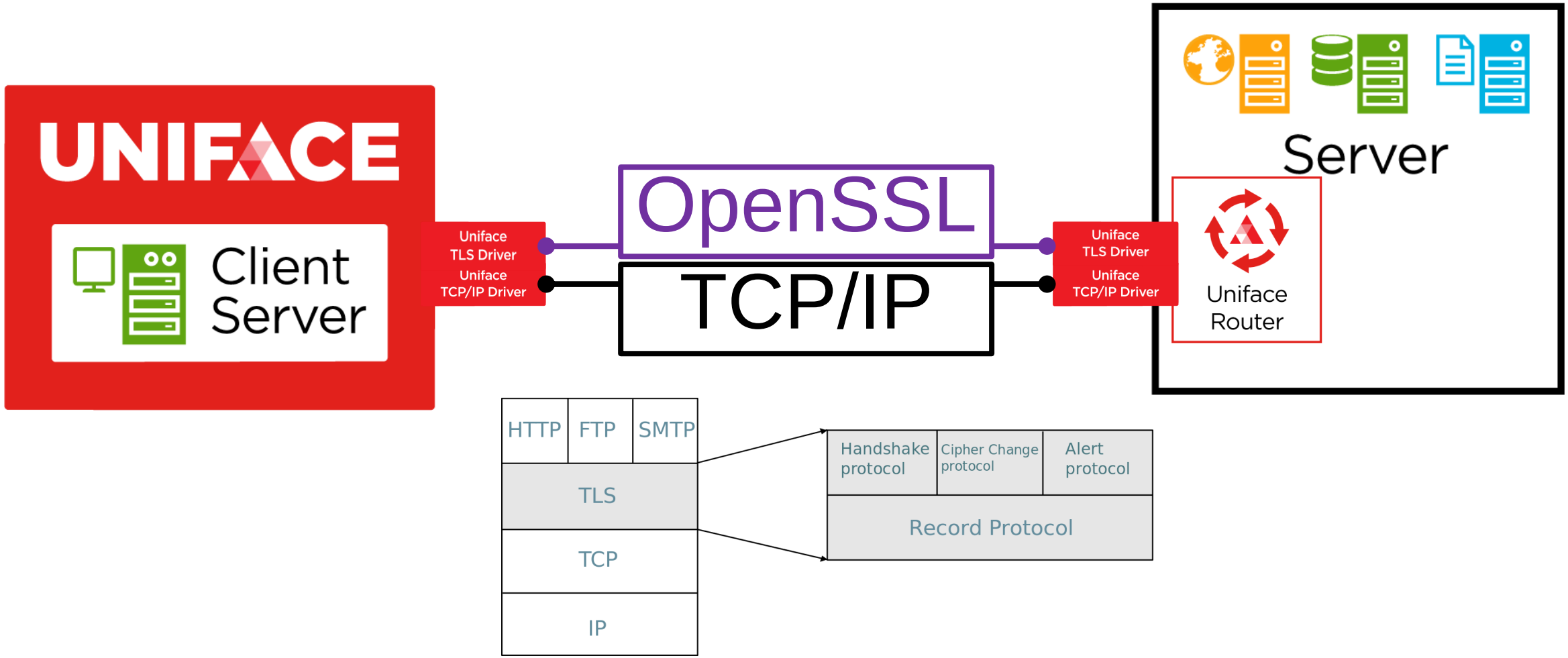
- ‘Swiss Army Knife’ of cryptography
- Backed by major organisations and government institutions
- Well maintained, and supported
- Excellent platform coverage
- openssl ciphers –v
  - Kx (Key Exchange algorithm)
  - Au (Authentication algorithm)
  - Enc (Encryption algorithm)
  - Mac (Message authentication code)

OpenSSL
Cryptography and SSL/TLS Toolkit

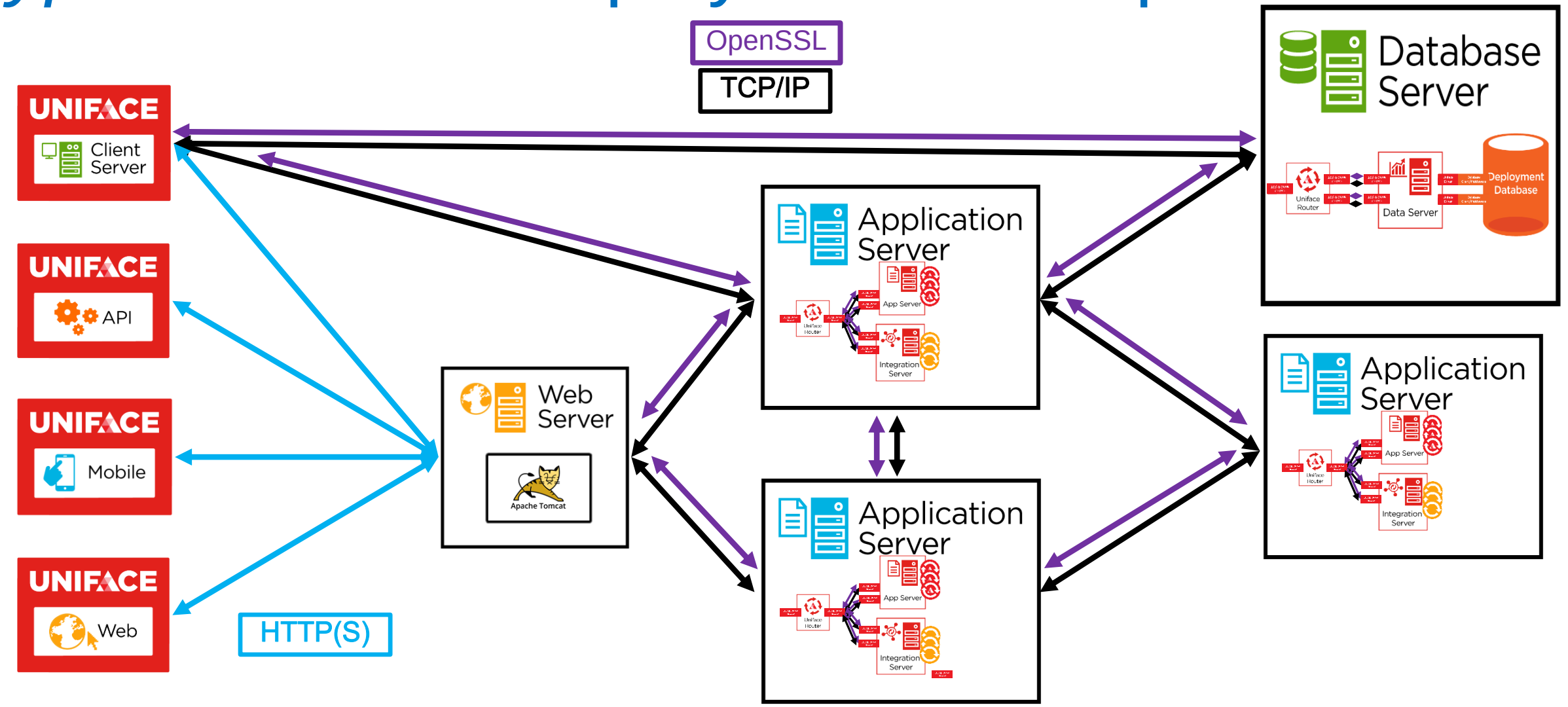
Familiar configuration

- Typical driver style approach
  - TLS:
  - USYS$TLS_PARAMS
- Connection profiles in [NET_SETTINGS]
- Line continuation (%\ ) is now implemented

TLS layer over TCP/IP, using OpenSSL



Typical Uniface Deployment Example



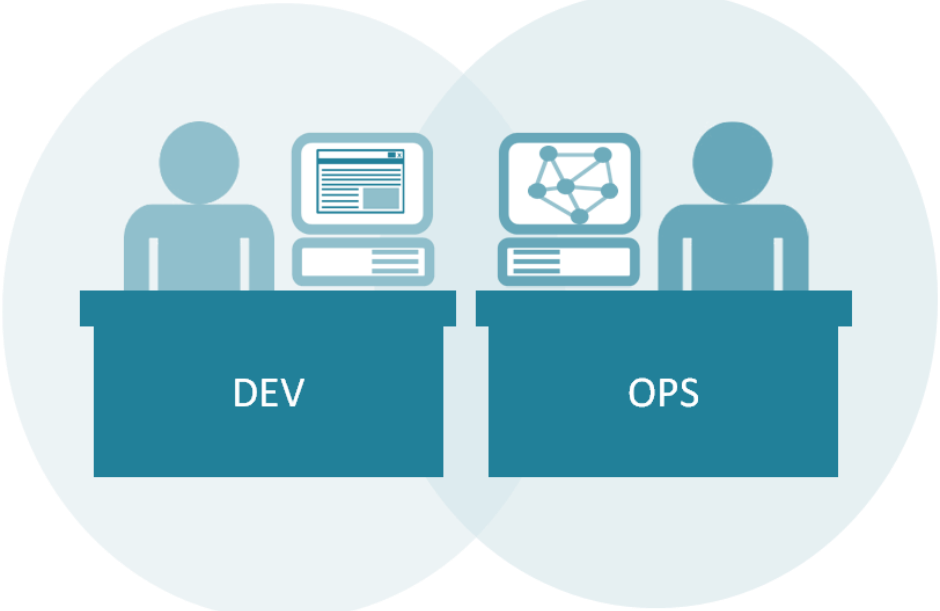
What does this mean for you?

Development

- Not much, development is *more or less* no change
  - Transaction size, client vs server processing *could* become a consideration

Operations

- Know what security, TLS and encryption is
- Know what encryption policies are required
- Know the pathscrambler and how to use it



Security is a shared responsibility

Implementation considerations

Using TLS will come with a performance penalty

- Encryption & decryption require additional processing power
- Different cyphers have different performance overheads
- Application behaviour will have an impact
- Deployment hardware can have an impact
- Published benchmarks are available
- Our testing reflects published OpenSSL benchmarks

PSK based TLS			Extra overhead by different sizes of data passed			
Server configuration	Network Connection	Scenario	10KB (1000x)	100KB (1000x)	1000KB (1000x)	10 000KB (1000x)
Exclusive userver	TCP	Activate	760 ms	3170 ms	29560 ms	535790 ms
	PSK-AES256-CBC-SHA	Activate	+12%	+13%	+11%	+15%
	PSK-AES256-CBC-SHA	DB	+10%	+16%	+10%	+21%
	PSK-AES128-CBC-SHA	DB	+16%	+15%	+21%	+20%
	PSK-3DES-EDE-CBC-SHA	DB	+104%	+143%	+160%	+141%
	PSK-RC4-SHA	DB	+8%	+12%	+18%	+18%

Ceritificate based TLS			Duration of different sizes of data passed through in ms			
Server configuration	Network Connection	Scenario	10KB (1000x)	100KB (1000x)	1000KB (1000x)	10 000KB (1000x)
Exclusive userver	TCP	Activate	760 ms	3170 ms	29560 ms	535790 ms
	DES-CBC3-SHA	Activate	+24	+87	+97	+92
	RC4-SHA	DB	+10	+13	+16	+18

YOUR APPLICATION WILL BE DIFFERENT!


Uniface TLS in action
UNIFACE

Thank You & Questions

UNIFACE

UNIFACE

uniface.com