TLS 1.3 – Minor Version, Major Change

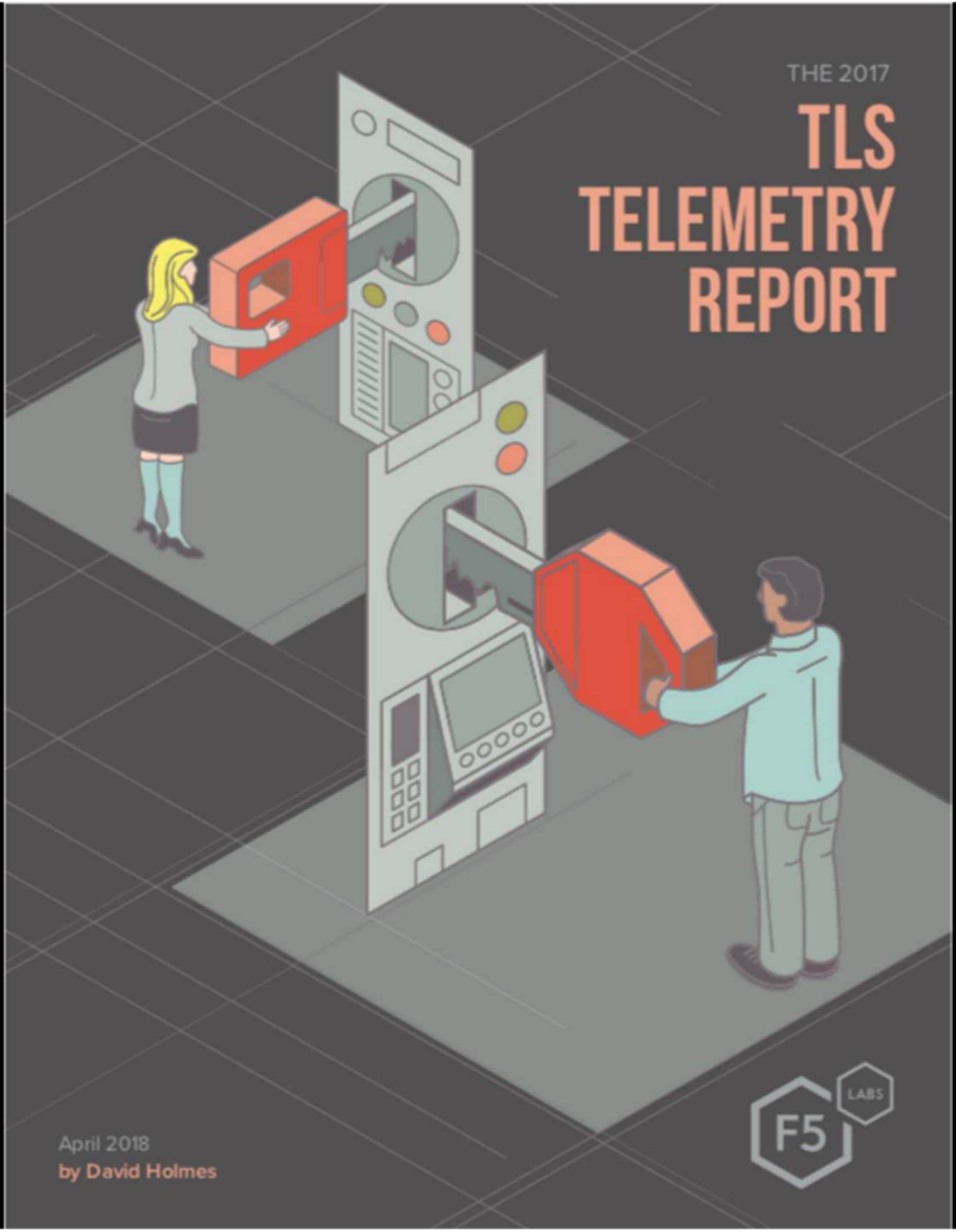
PRESENTED BY:
Brett Smith - Senior Systems Engineer
brett@f5.com

Thank You

Agenda

- F5 Labs: TLS Telemetry Report
- TLS 1.3
- What does this mean?

It’s all about Keys!



THE 2017

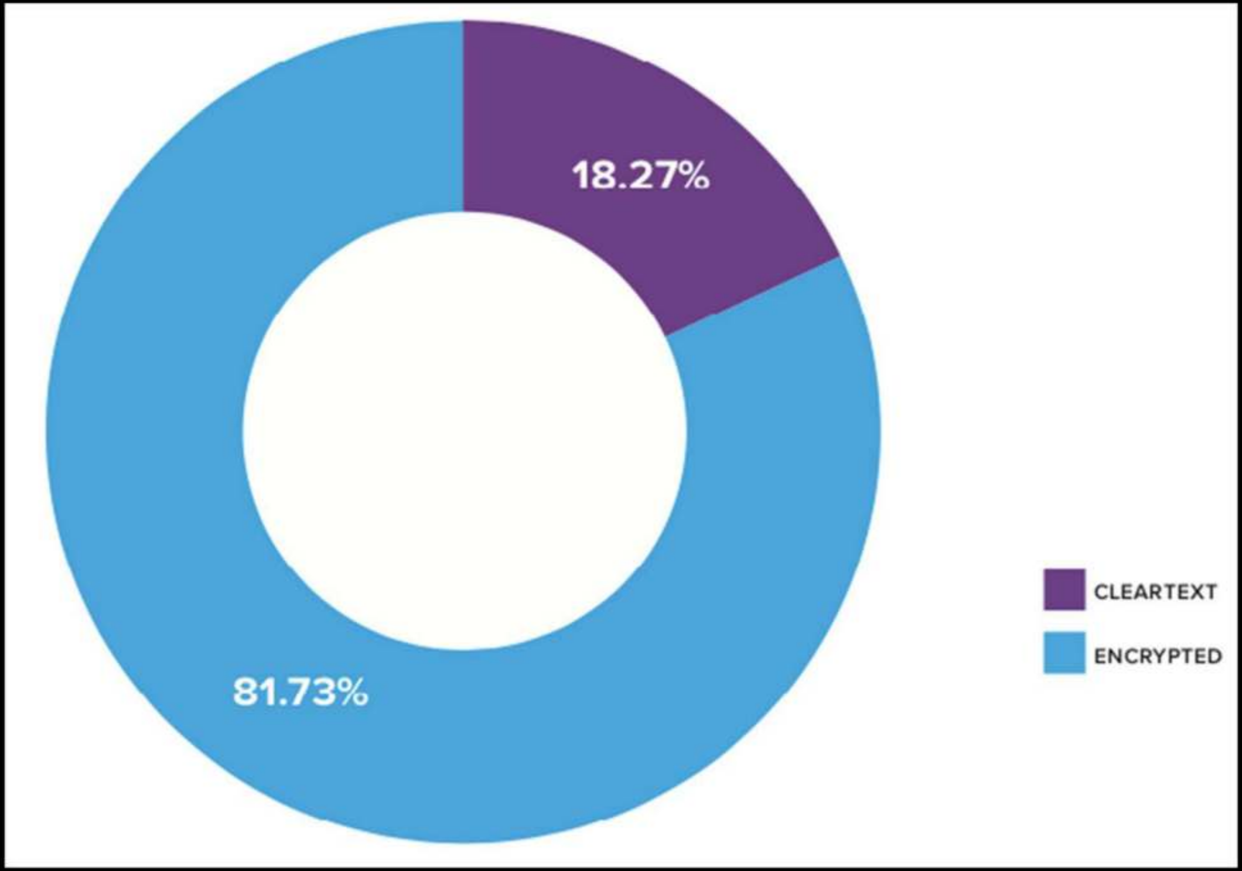
TLS TELEMETRY REPORT

April 2018

by David Holmes

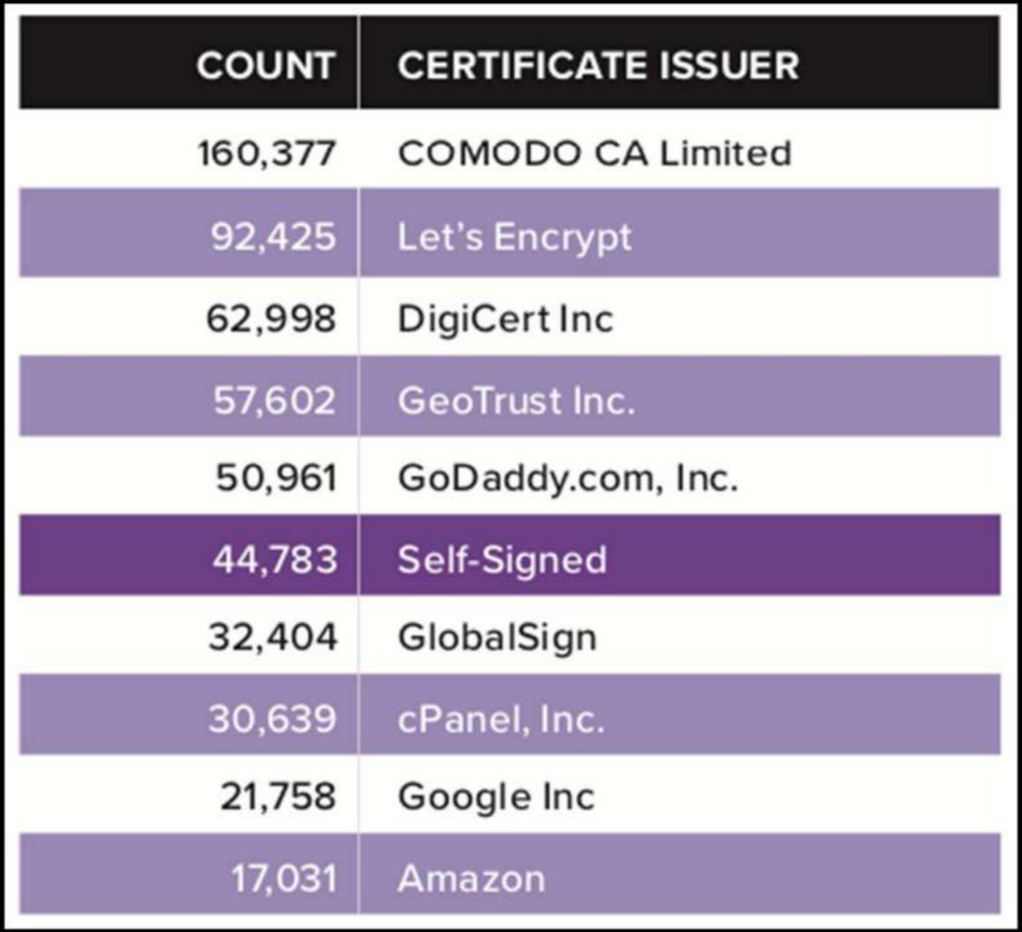
Encrypted HTTP page loads > 80%

Is TLS is now the most import protocol on the Internet?



source: telemetry.mozilla.org

Top 10 Certificate Authorities

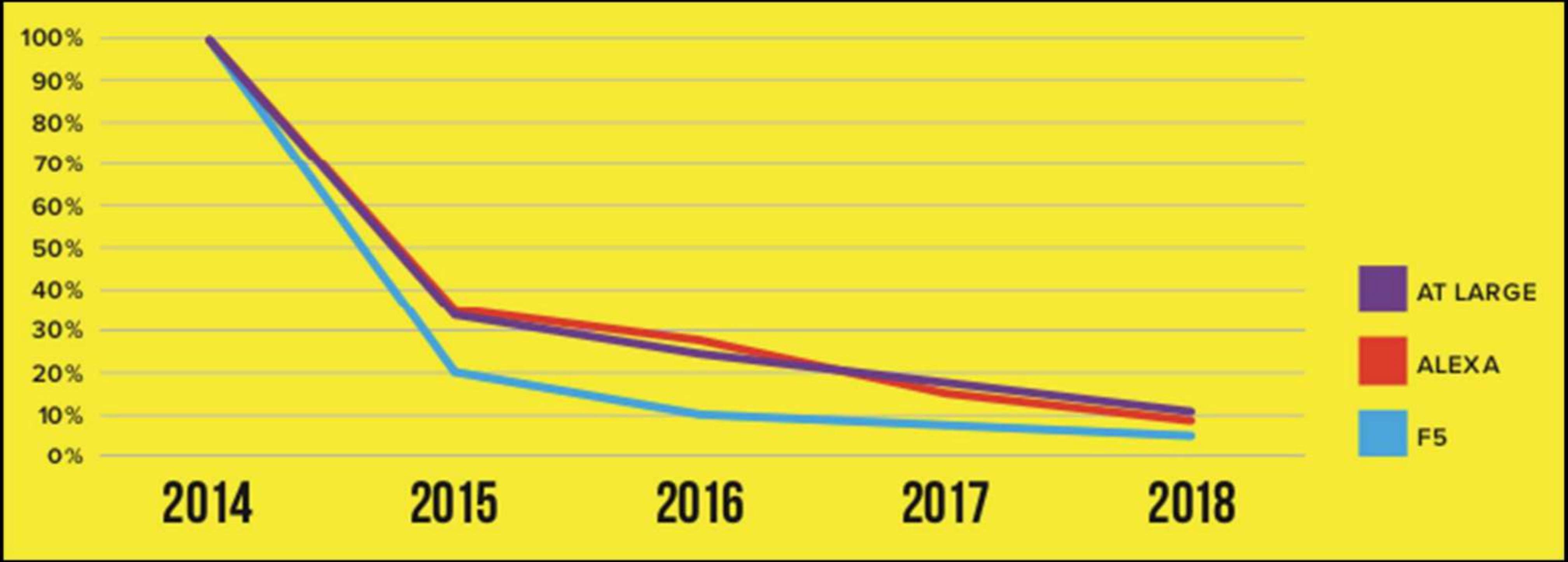


COUNT	CERTIFICATE ISSUER
160,377	COMODO CA Limited
92,425	Let's Encrypt
62,998	DigiCert Inc
57,602	GeoTrust Inc.
50,961	GoDaddy.com, Inc.
44,783	Self-Signed
32,404	GlobalSign
30,639	cPanel, Inc.
21,758	Google Inc
17,031	Amazon

- Let's Encrypt, the power of free.
- Comodo retains the top spot and has for a decade.

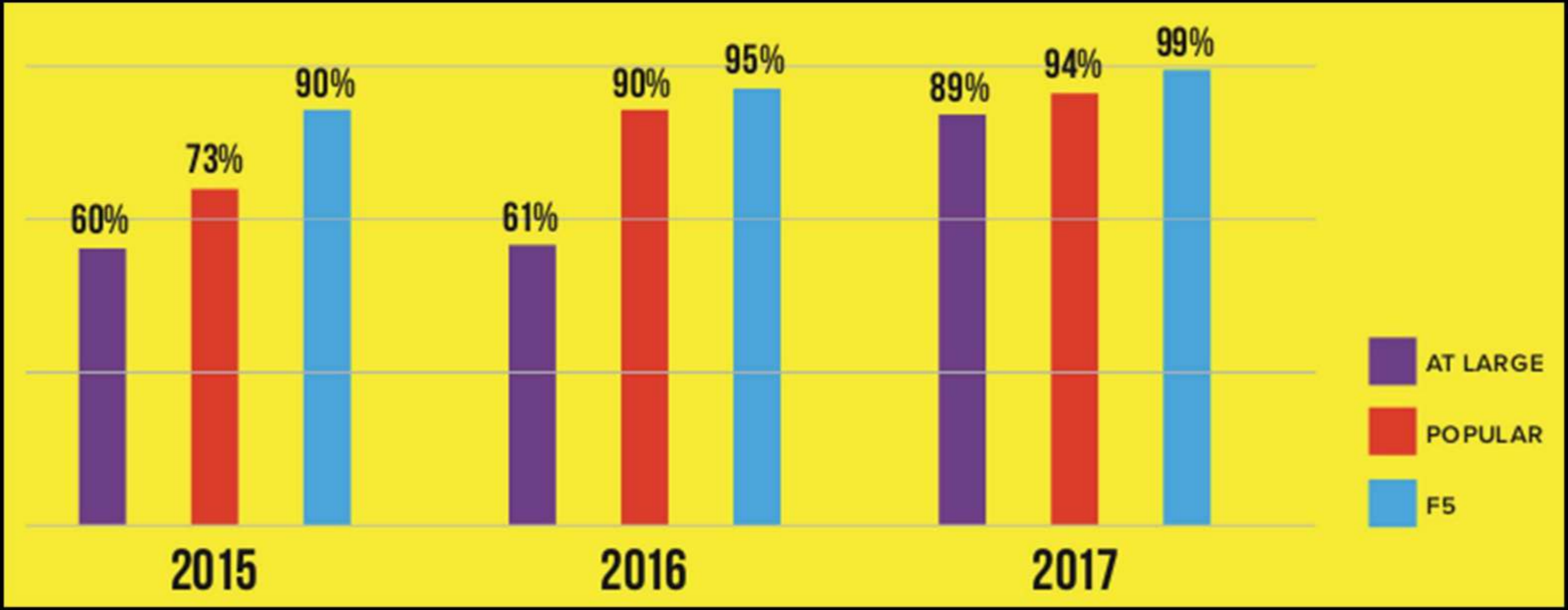
SSLv3 is dying a slow death

STOP using SSLv3!



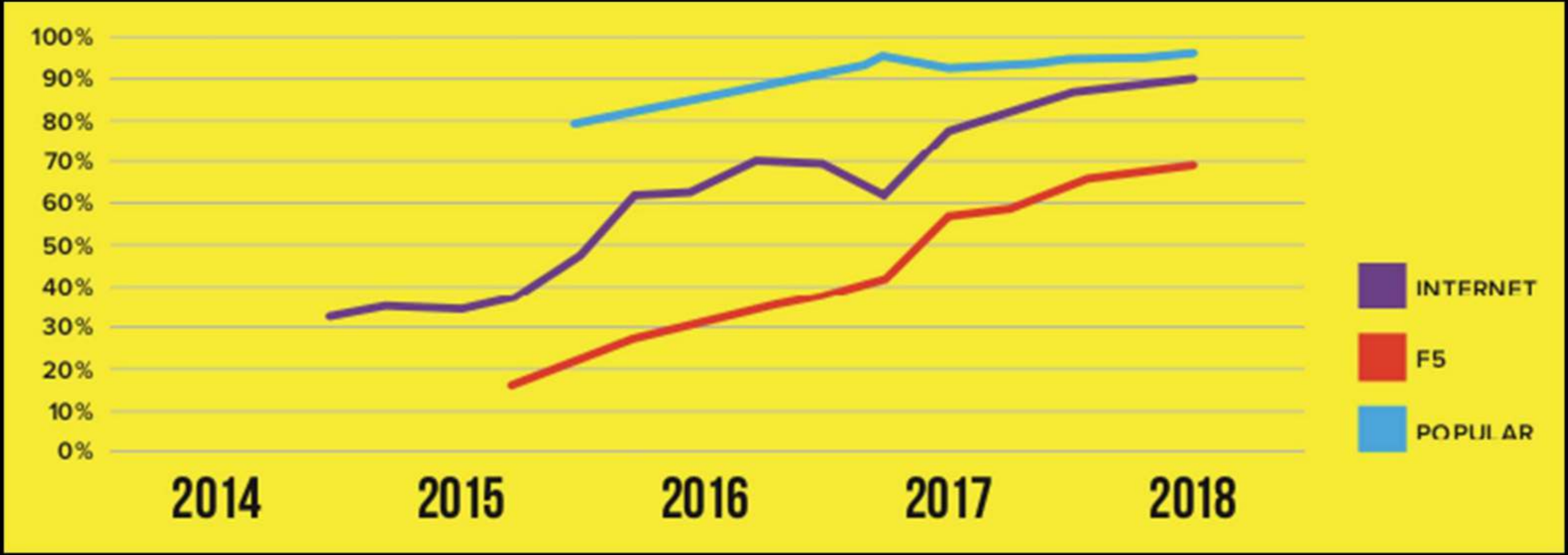
TLS 1.2 is peaking

At the beginning of 2018 it had risen to 89%.



Perfect Forward Secrecy is charging forward

What does this mean for visibility?

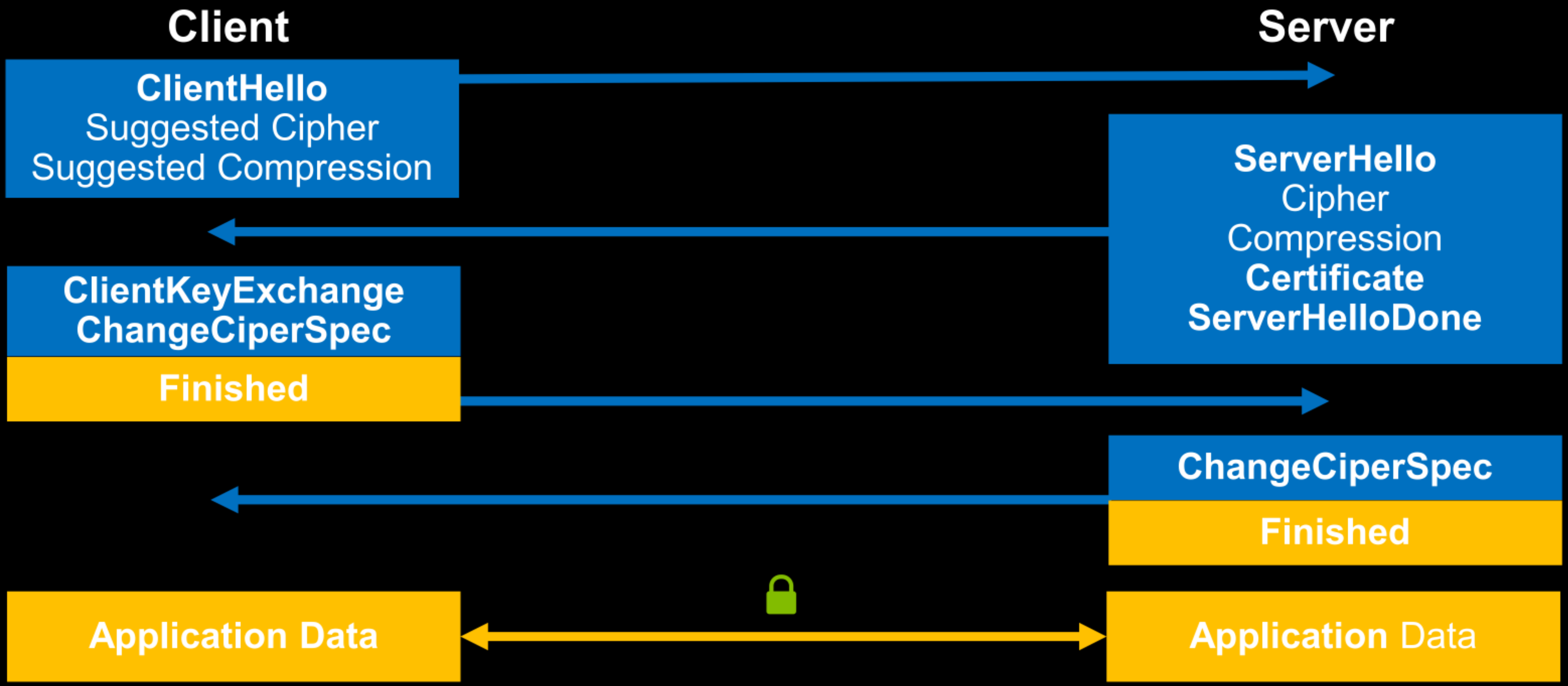


TLSv1.3

SSL/TLS History

- SSLv1.0 – Never released
- SSLv2.0 – February 1995
- SSLv3.0 – RFC 6101 November 1996
- TLSv1.0 – RFC 2246 January 1999
- TLSv1.1 – RFC 4346 April 2006
- TLSv1.2 – RFC 5246 August 2008
- TLSv1.3 – RFC 8446 August 2018

Revision TLSv1.2 – Handshake (Static RSA)



Client

Server

ClientHello
Suggested Cipher
Suggested Compression

ServerHello
Cipher
Compression
Certificate
ServerHelloDone

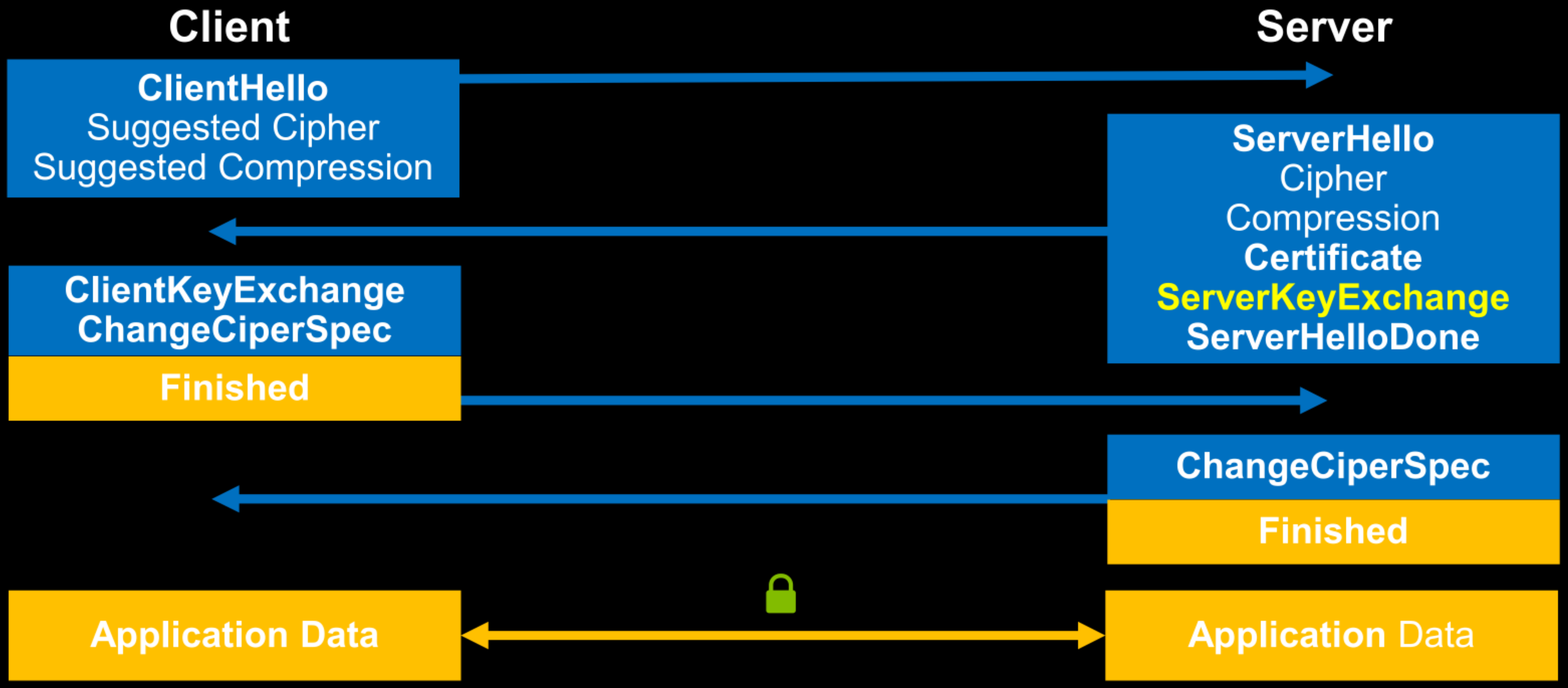
ClientKeyExchange
ChangeCiperSpec
Finished

ChangeCiperSpec
Finished

Application Data

Application Data

Revision TLSv1.2 – Handshake ({EC}DHE)



Client

Server

ClientHello
Suggested Cipher
Suggested Compression

ServerHello
Cipher
Compression
Certificate
ServerKeyExchange
ServerHelloDone

ClientKeyExchange
ChangeCiperSpec
Finished

ChangeCiperSpec
Finished

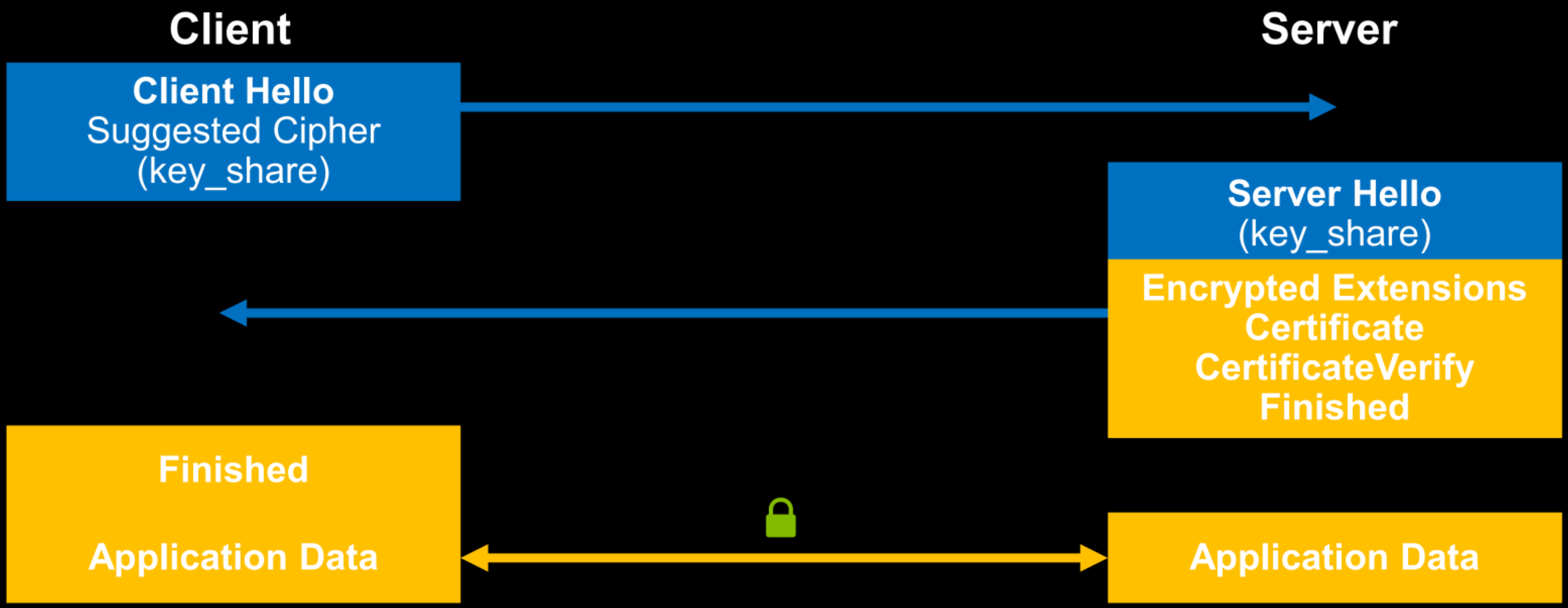
Application Data

Application Data

* DHE and ECDHE provides Forward Secrecy

TLSv1.3 – Handshake ({EC}DHE) only

TLSv1.3 – More Privacy, Less Latency



Client

Server

Client Hello
Suggested Cipher
(key_share)

Server Hello
(key_share)

Encrypted Extensions
Certificate
CertificateVerify
Finished

Finished

Application Data

Application Data

1-RTT (Round Trip Time)

TLSv1.3 Handshake Changes

Removed

- Compression
- ChangeCipherSpec
- ServerHelloDone
- Renegotiation

Moved

- ClientKeyExchange => key_share extension
- ServerKeyExchange => key_share extension

Improved Security

TLS1.3 removes insecure features from TLS1.2

Removed

- SHA-1
- RC4
- DES
- 3DES
- AES-CBC
- MD5

Removed

- Arbitrary Deffe-Hellman Group
- EXPORT Ciphers

TLSv1.3 Cipher Suites

Is that it?

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_AES_128_CCM_8_SHA256

TLS1.3 Browser Support

Support

- Chrome 56+
- Chrome for Android
- Firefox 52+
- Safari 11.1+ (disabled by default)

Not Supported

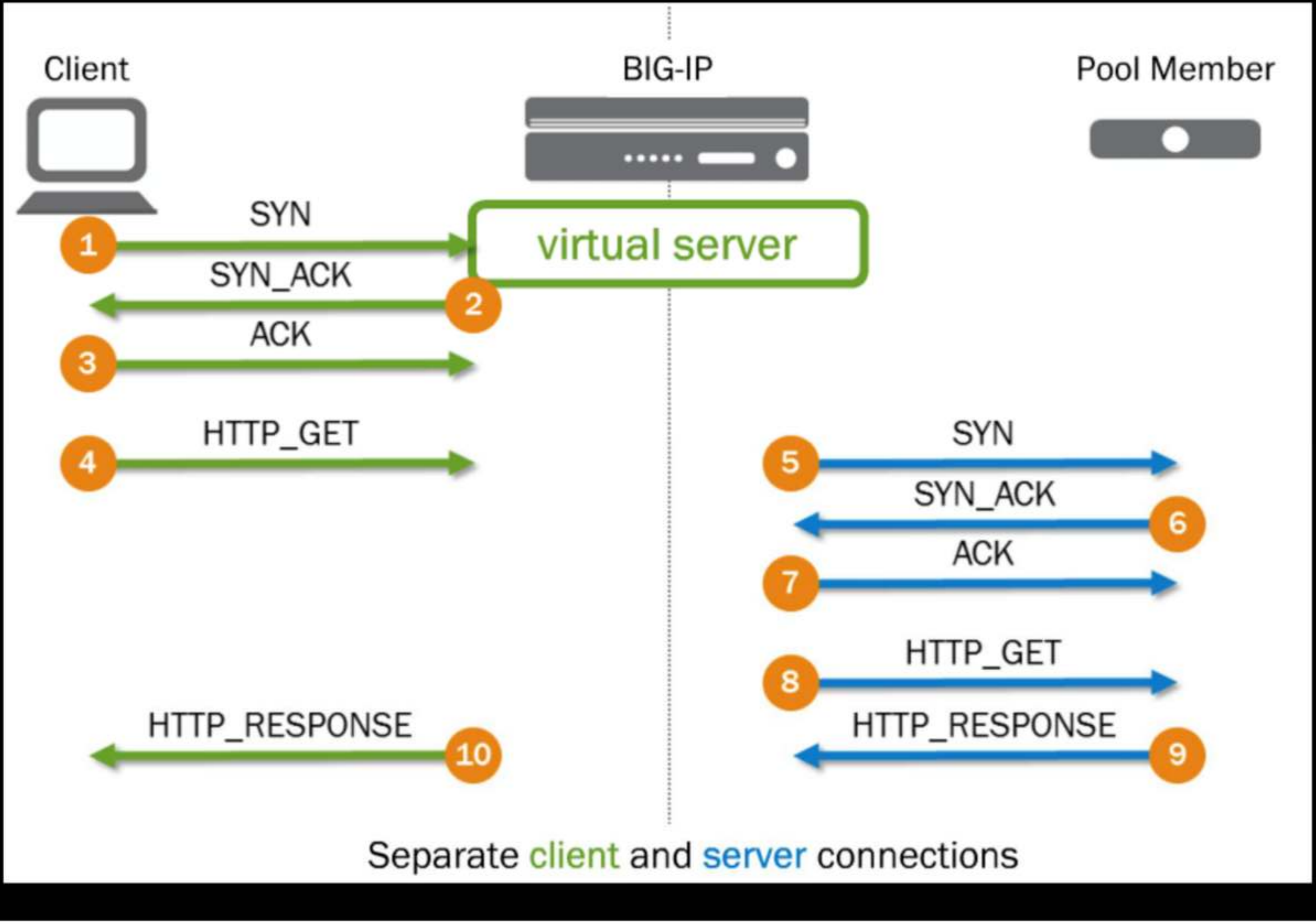
- IE
- Edge
- Opera

What does this mean?

Less visibility, but more secure??

- No more non-ephemeral key exchange (Static RSA, DH, ECDH)
- Much less information is available in a TLSv1.3 capture. How do you troubleshoot?
- Is it more secure?
- **TLSv1.3 is going to make life ‘interesting’.**

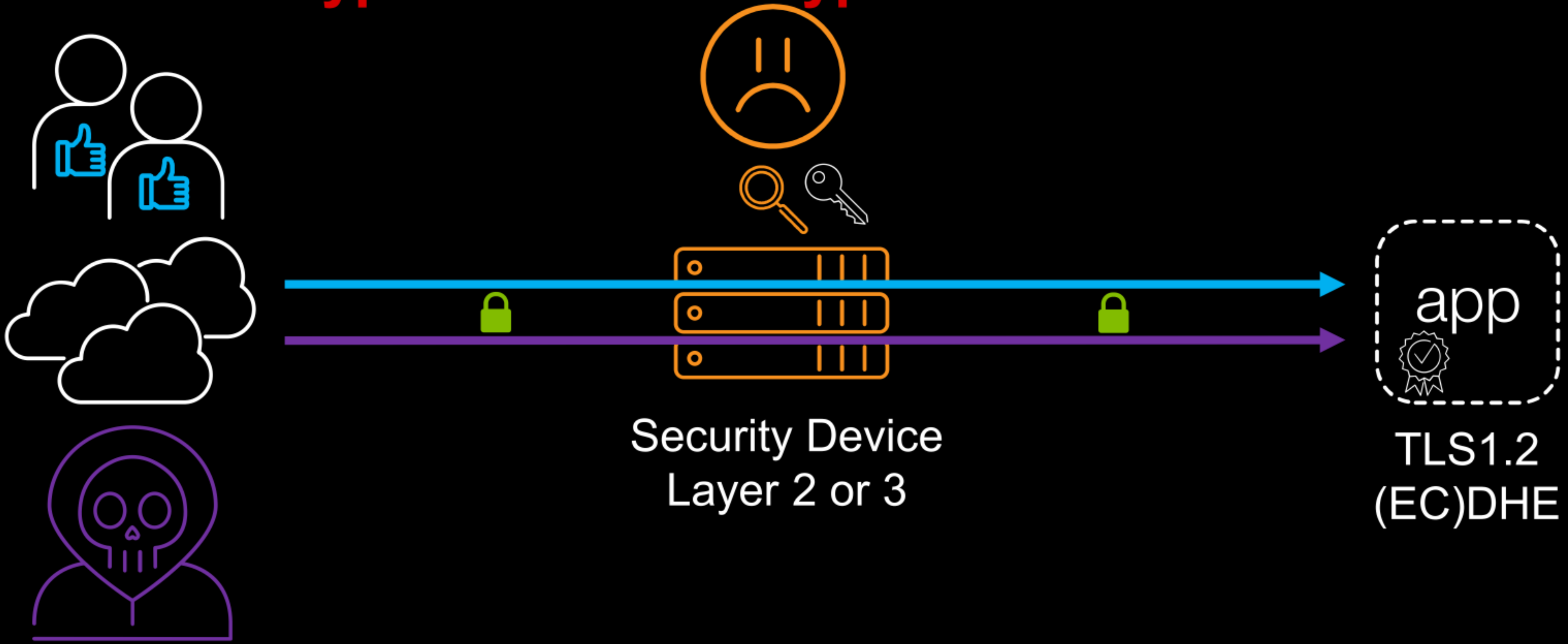
What is a Full Proxy?



Separate client and server connections

Example: Inbound Use-case

Passive Decryption = No Decryption

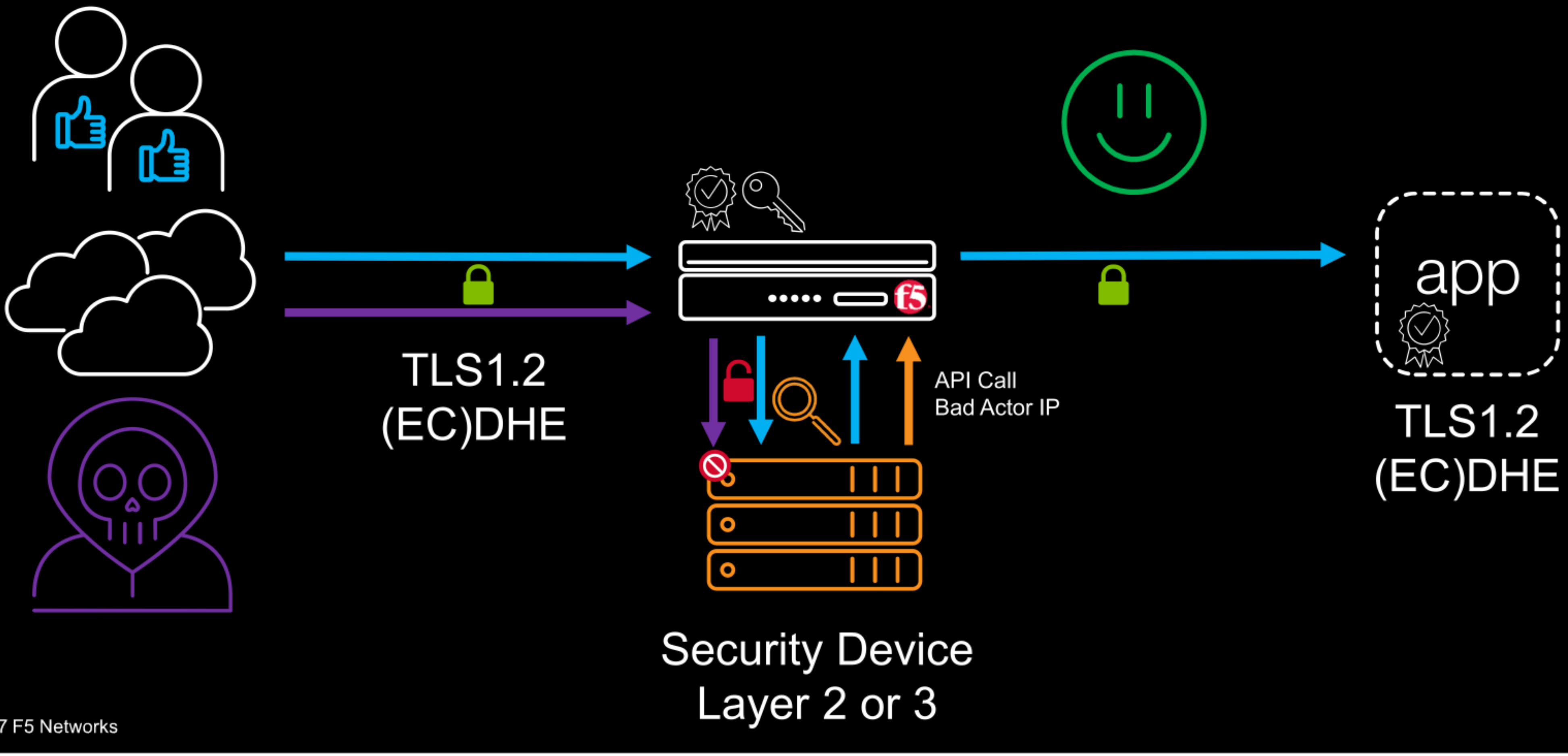


Security Device
Layer 2 or 3

TLS1.2
(EC)DHE

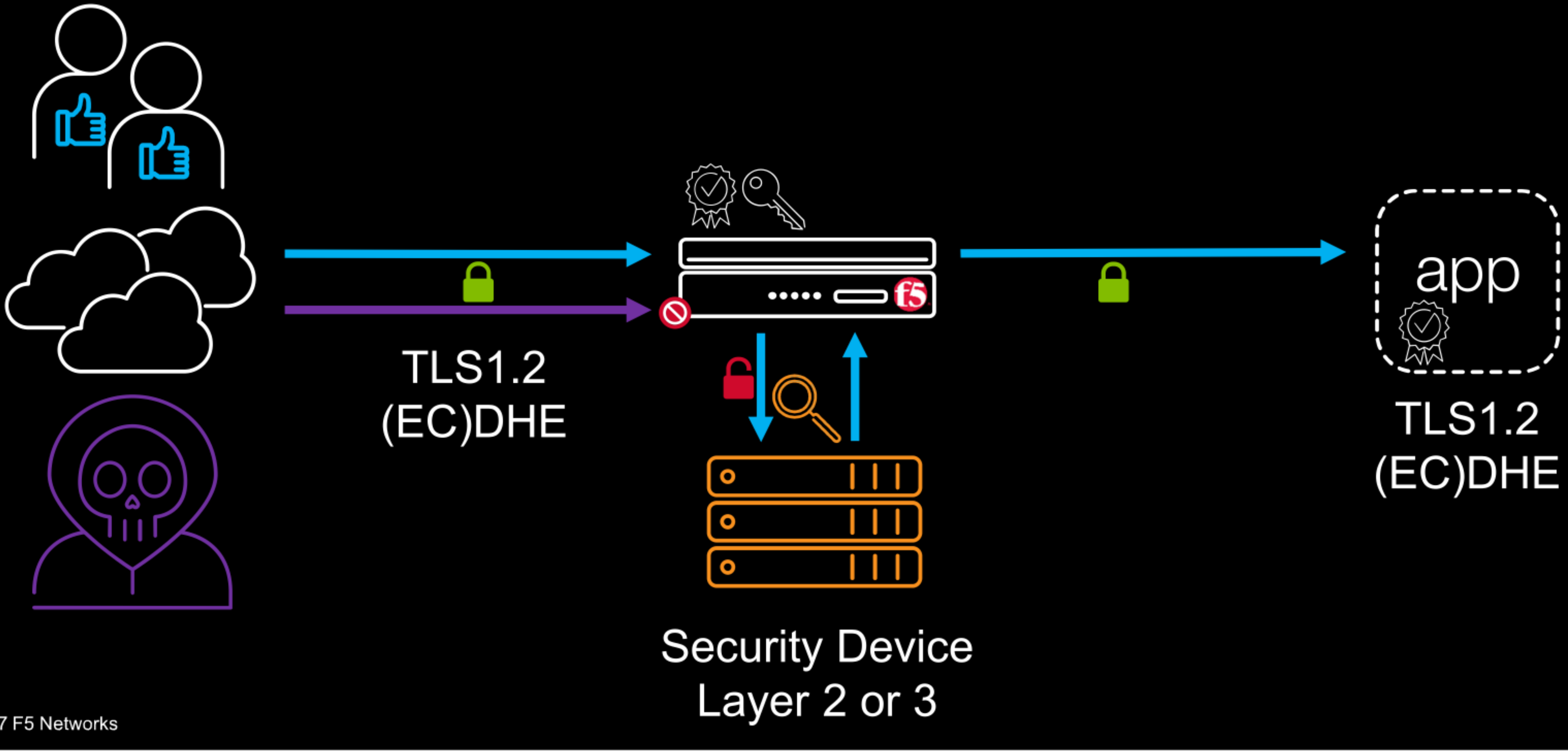
Example: Inbound Use-case

BIG-IP Proxy – SSL Visibility



Example: Inbound Use-case

BIG-IP Proxy – SSL Visibility



Summary

- Disable SSLv3
- Use/Preference Ephemeral Ciphers
- Use a Full Proxy architecture to enhance your security and visibility

Tools

- SSL Labs: https://www.ssllabs.com/ssltest/
- Bad SSL: https://badssl.com/
- testssl.sh: https://testssl.sh/