RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: ACB-W09

The Network Is Going Dark: Why Decryption Matters for SecOps

Jesse Rothstein

Co-Founder and CTO
ExtraHop Networks
@Jesse_Rothstein

Joshua Northrup

Manager of Monitoring and Automation
Fiserv

Introduction

Jesse Rothstein

Jesse is responsible for the technical direction and architecture of the ExtraHop platform. Rothstein co-founded ExtraHop in 2007. Before ExtraHop, Jesse held a six-year tenure at F5 Networks where he was a Senior Software Architect and co-inventor of the TMOS platform at F5.

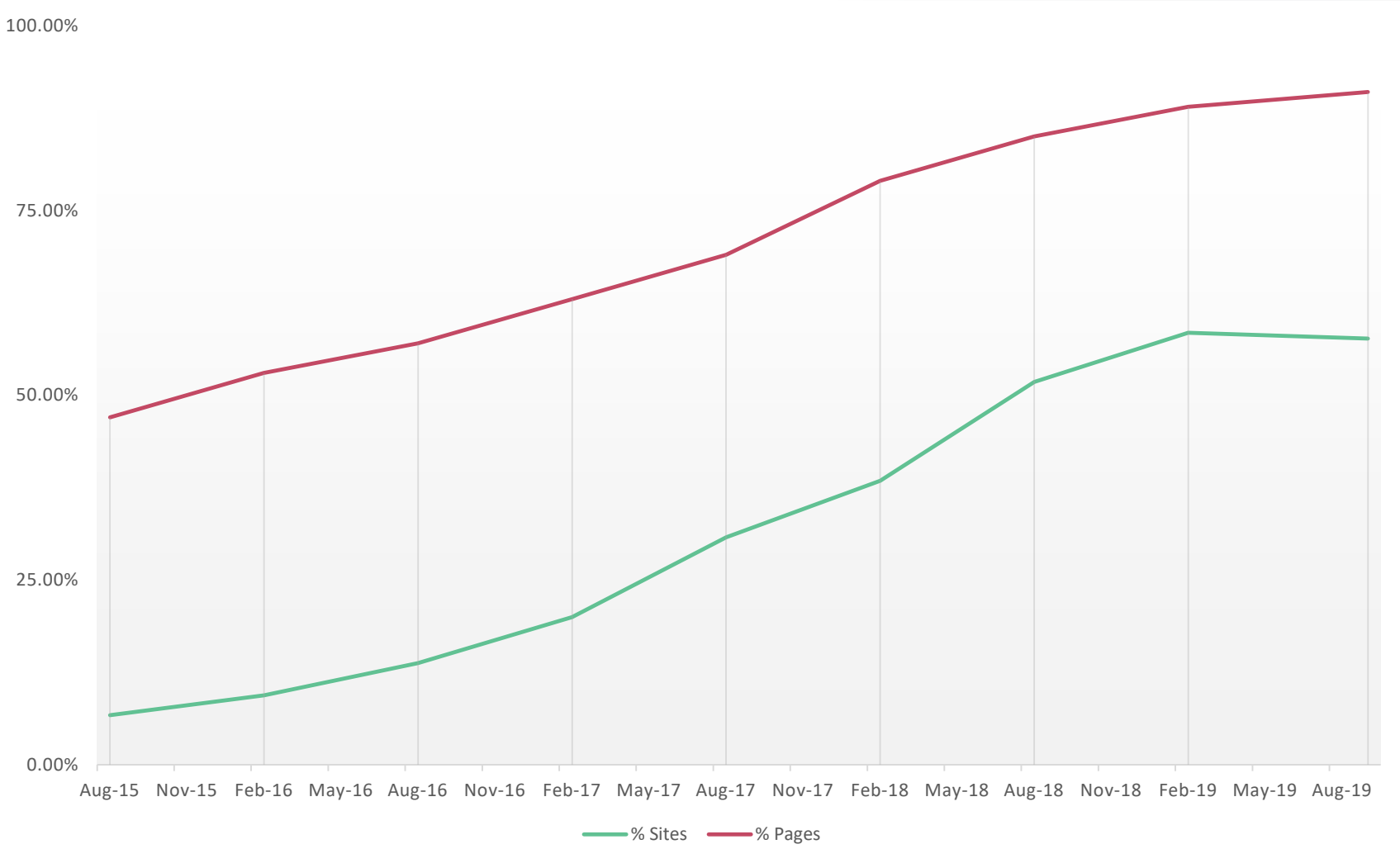
Joshua Northrup

Josh planned, architected and implemented the ExtraHop deployment at Fiserv, one of the world's largest payment clearinghouses. At Fiserv, Northrup designed and implemented an intelligent monitoring and self-healing automation framework.

Agenda

- Encryption Trends
- TLS 1.3
- Network Detection
- Visibility Challenges
- Traffic Analysis
- Decryption
- Fiserv Case Study
- Next Steps

Encryption Trend



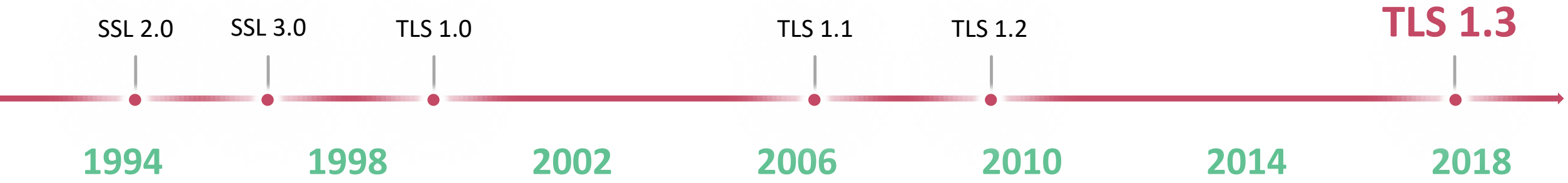
91% of Pages Loaded over HTTPS in Chrome

58% of Top Sites Redirect to HTTPS

Google Transparency Report, "HTTPS encryption on the web"
Scott Helme, "Top 1 Million Analysis", September, 2019

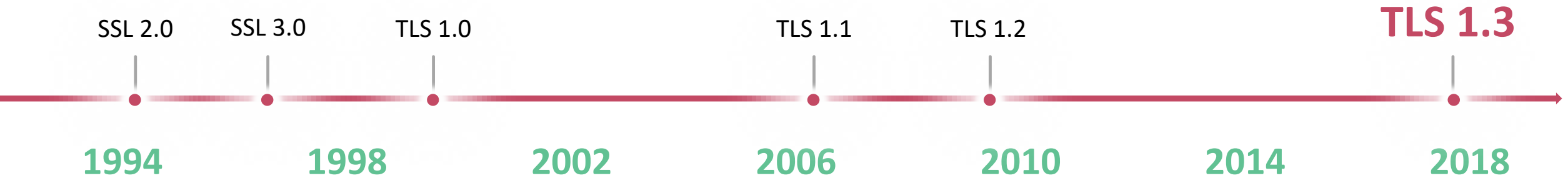
TLS 1.3 Is Here

- Chrome version 65 (March 2018)
- Firefox version 60 (May 2018)
- Java 11 (Sept 2018)
- OpenSSL 1.1.1 (Sept 2018)
- Apache 2.4.37 (Oct 2018)
- Go 1.13 (Sept 2019)
- Apple SecureTransport (early 2019)
- Microsoft Edge 79 (mid-Jan 2020)
- Windows 10 version 1909 (Nov 2019) (experimental only)

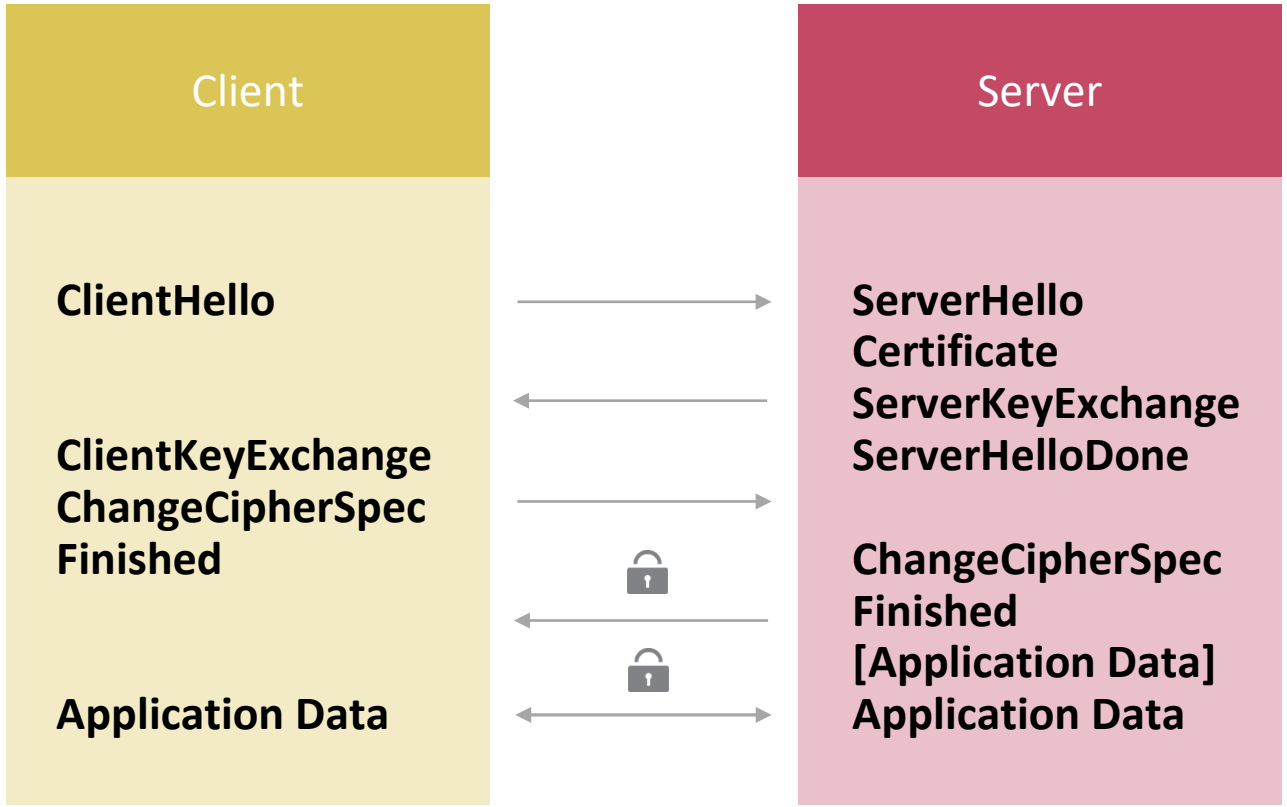


TLS 1.3 Highlights

- Faster handshakes
- No obsolete ciphers or hashes
- No compression or renegotiation
- Downgrade protection
- Encrypted certificates
- Perfect Forward Secrecy

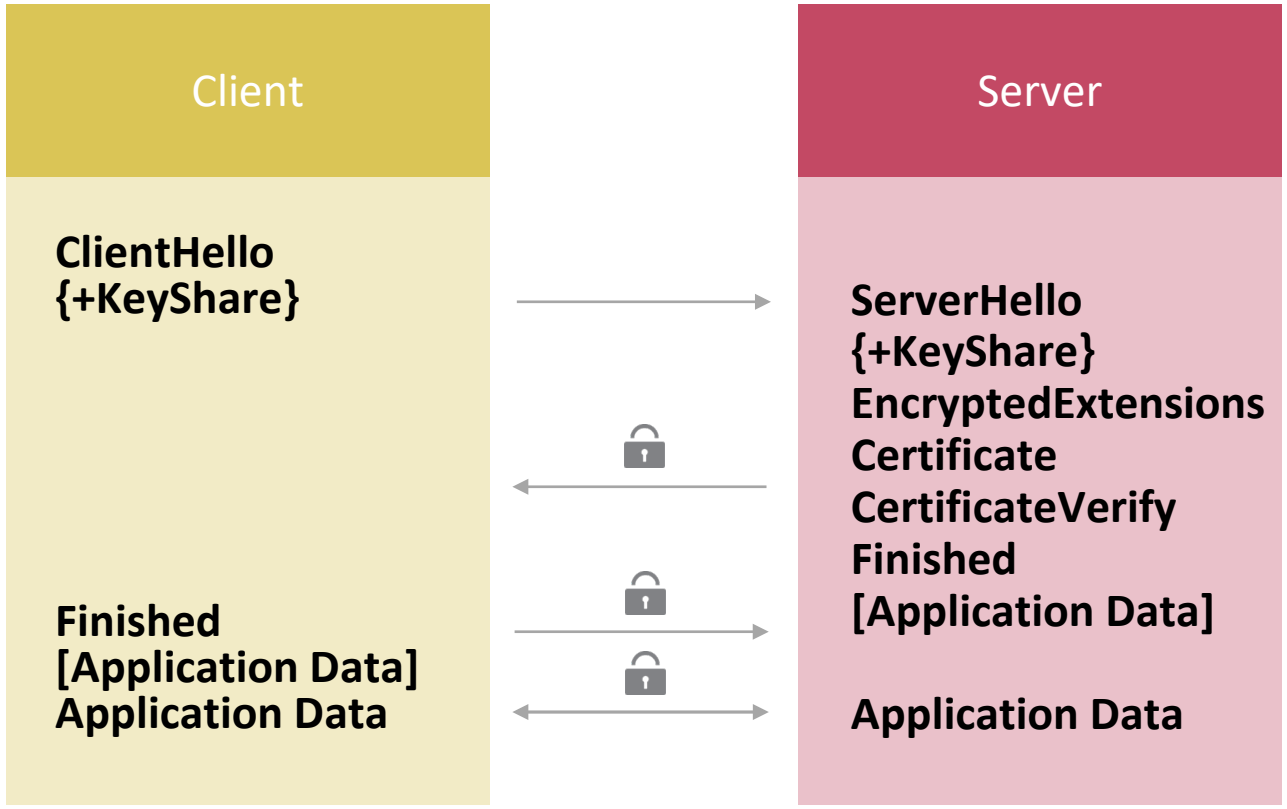


TLS 1.2 Handshake



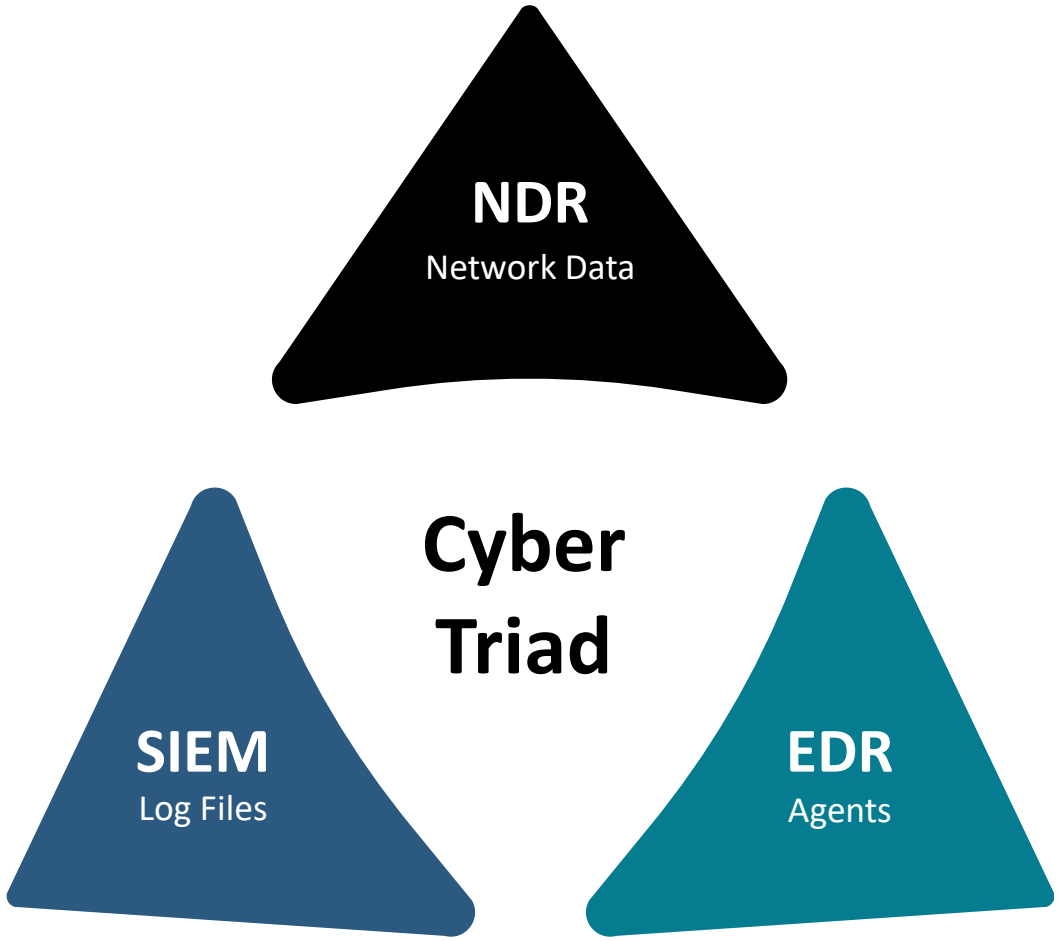
2-RTT handshake

TLS 1.3 Handshake



1-RTT handshake

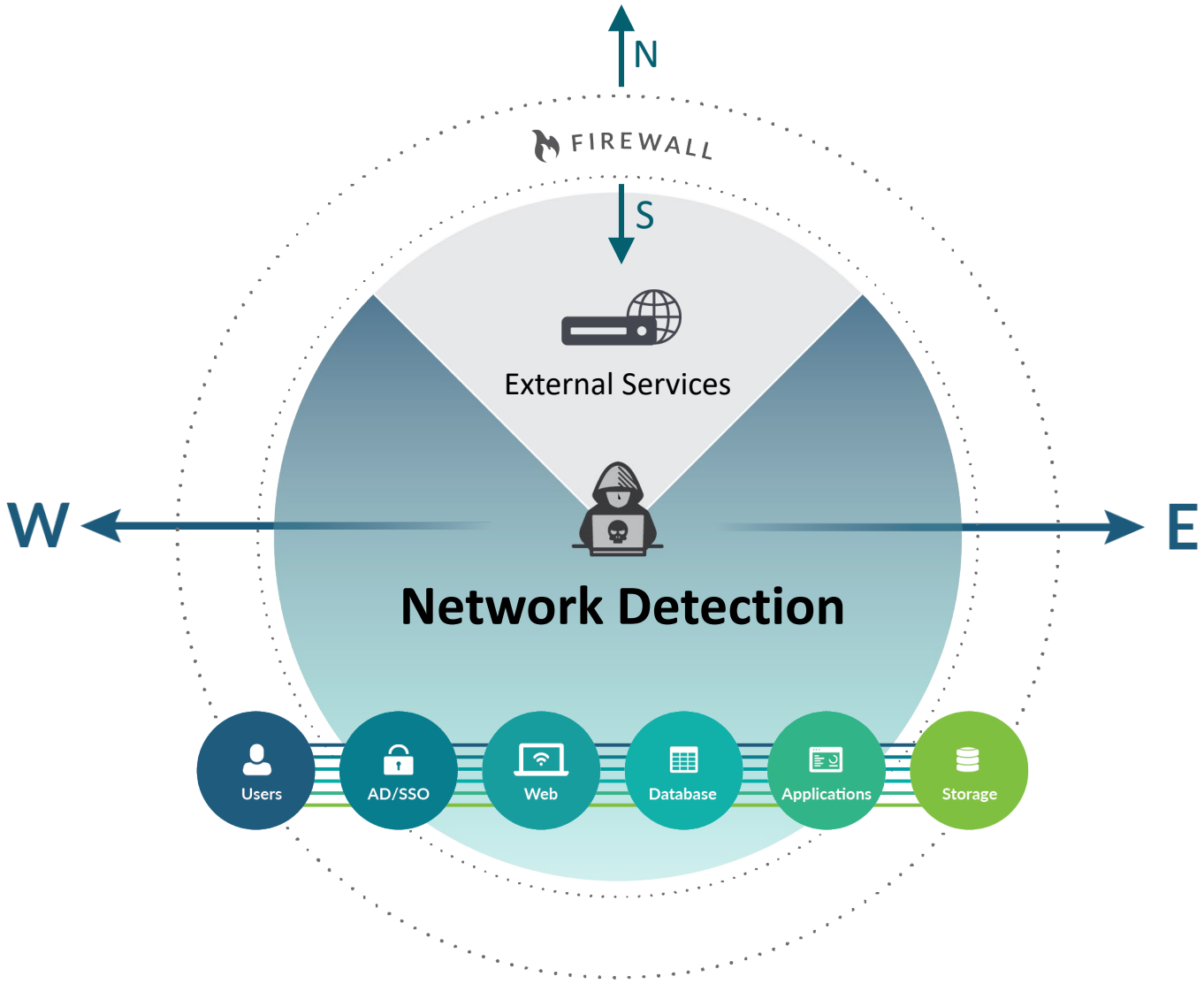
Why Network Detection?



> Network-based detection tools got the highest levels of satisfaction when compared against other detection approaches.

2019 SANS SOC SURVEY RESULTS

North-South vs. East-West



NORTH-SOUTH

Command & Control

Exfiltration

Initial Access

EAST-WEST

Discovery

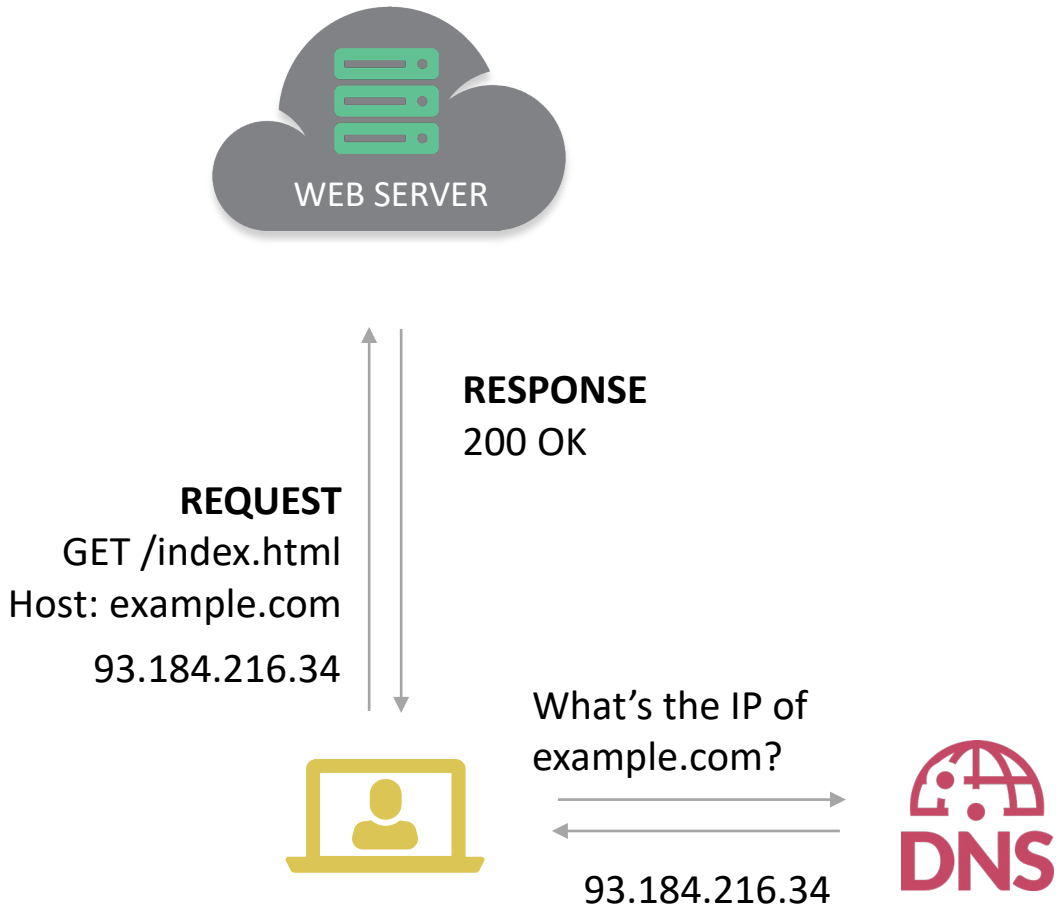
Credential Access

Lateral Movement

Collection

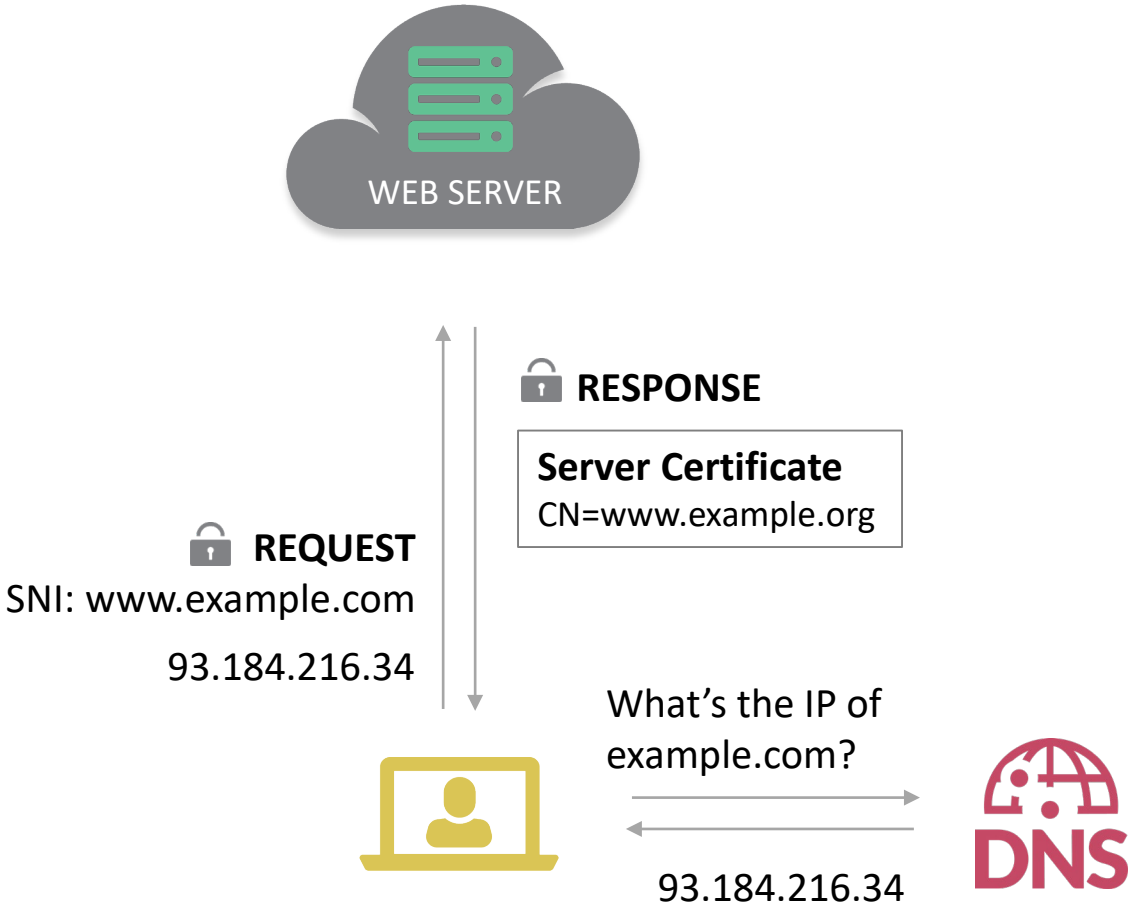
Privilege Escalation

North-South Visibility: HTTP



Unencrypted traffic == complete visibility

North-South Visibility: HTTPS (TLS 1.2)

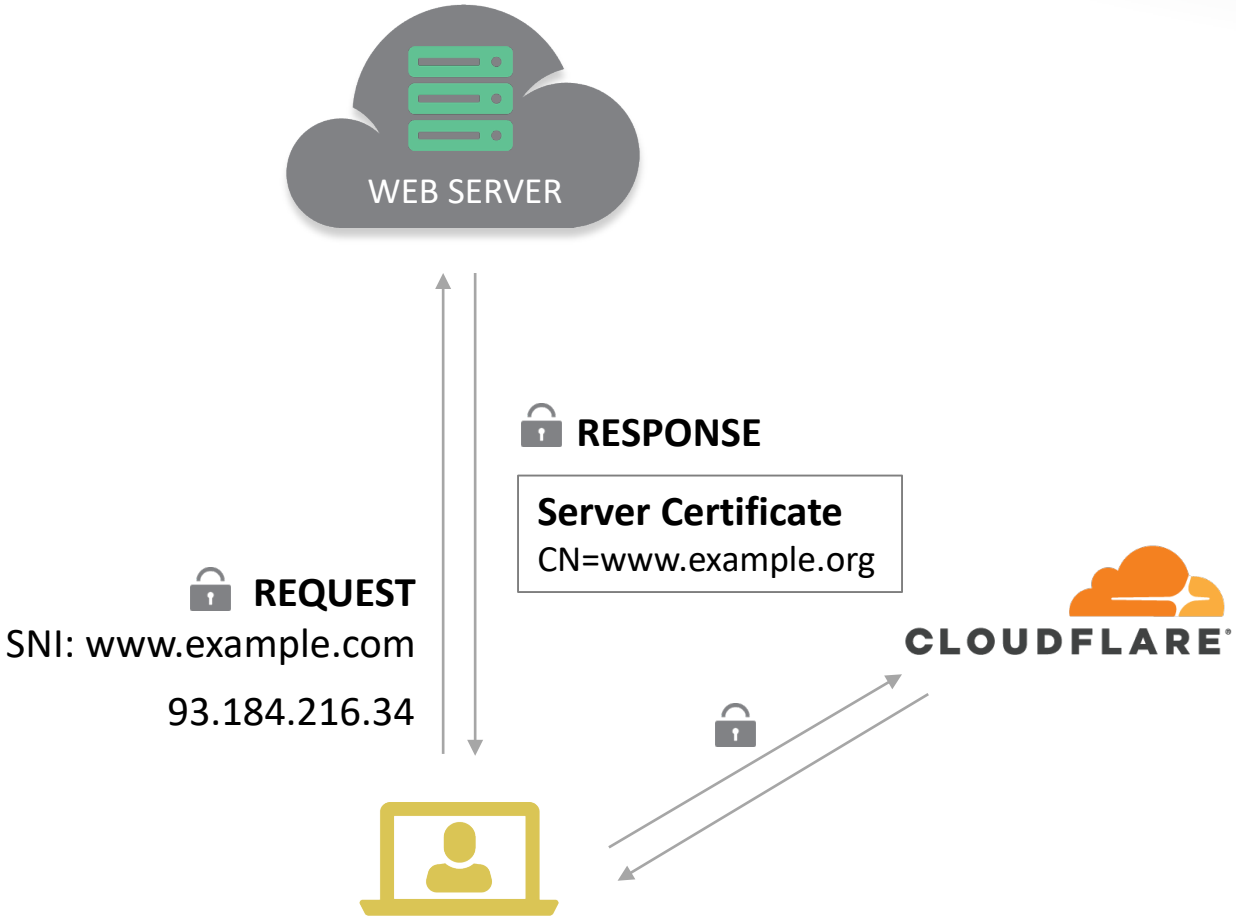


Good visibility through DNS, SNI, and Server Certificate

X.509 Certificate

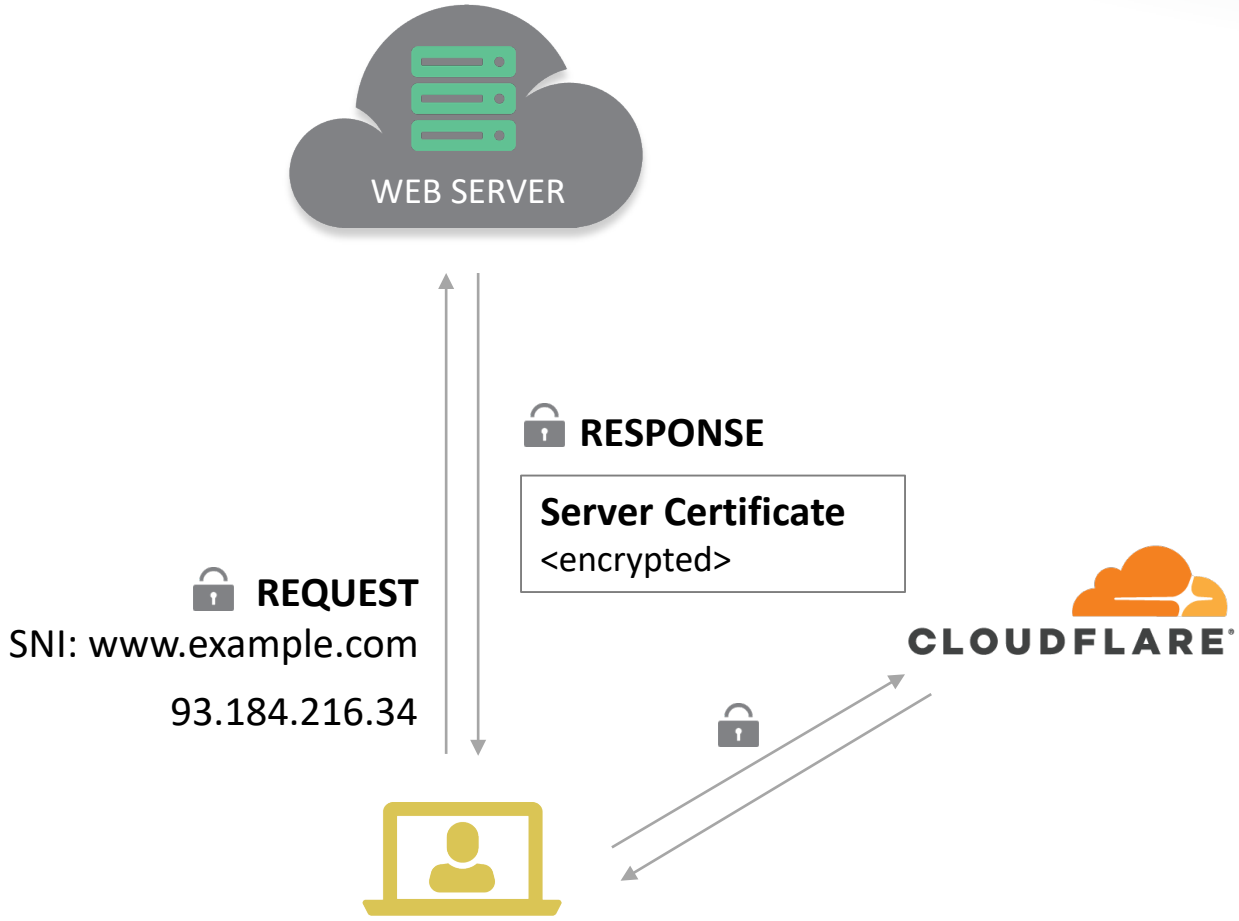
Server Certificate
Version: 3 (0x2)
Serial Number: 0f:d0:78:dd:48:f1:a2:bd:4d:0f:2b:a9:6b:60:38:fe
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
Validity
  Not Before: Nov 28 00:00:00 2018 GMT
  Not After : Dec 2 12:00:00 2020 GMT
Subject: C=US, ST=California, L=Los Angeles, O=Internet Corporation for Assigned Names and Numbers, OU=Technology, CN=**www.example.org**
Public Key Algorithm: rsaEncryption (2048 bit)
X509v3 extensions:
  X509v3 Authority Key Identifier:
    keyid:0F:80:61:1C:82:31:61:D5:2F:28:E7:8D:46:38:B4:2C:E1:C6:D9:E2
  X509v3 Subject Key Identifier:
    66:98:62:02:E0:09:91:A7:D9:E3:36:FB:76:C6:B0:BF:A1:6D:A7:BE
  X509v3 Subject Alternative Name:
    DNS:www.example.org, DNS:example.com, DNS:example.edu, DNS:example.net, DNS:example.org, DNS:www.example.com, DNS:www.example.edu, DNS:www.example.net

North-South Visibility: HTTPS (TLS 1.2) + DoH



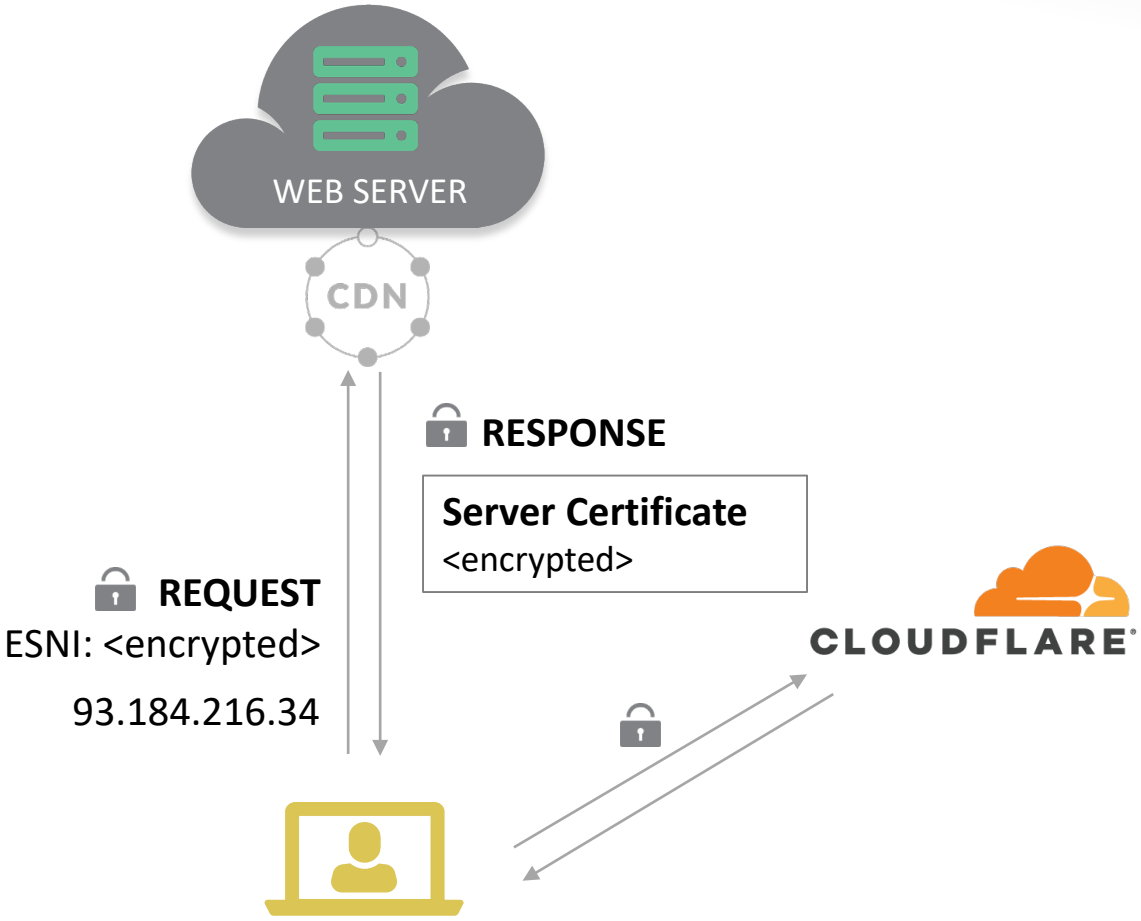
Some visibility through SNI and Server Certificate

North-South Visibility: HTTPS (TLS 1.3) + DoH



Limited visibility through SNI

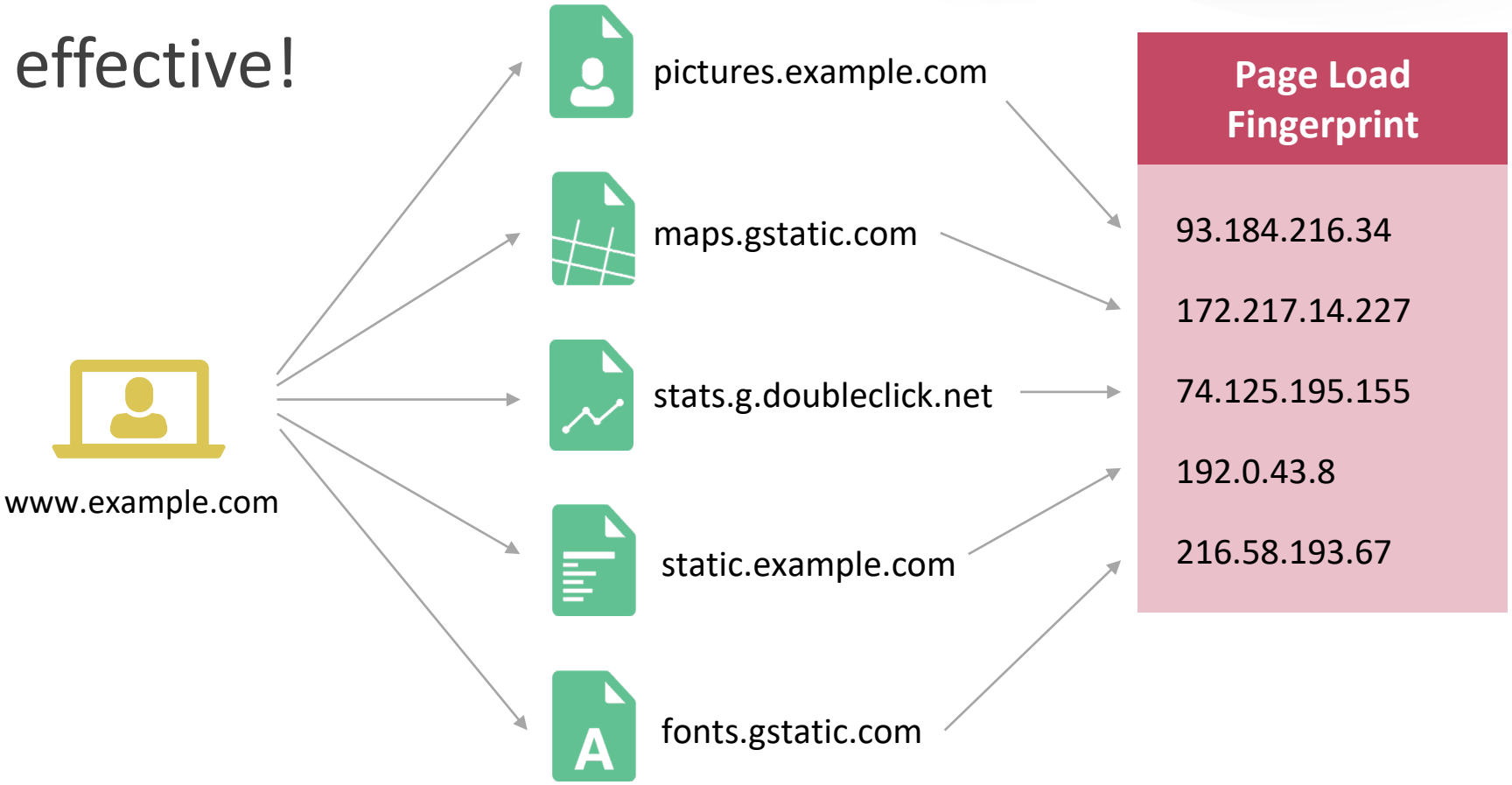
North-South Visibility: HTTPS (TLS 1.3) + DoH + ESNI



Very limited visibility through IP addresses

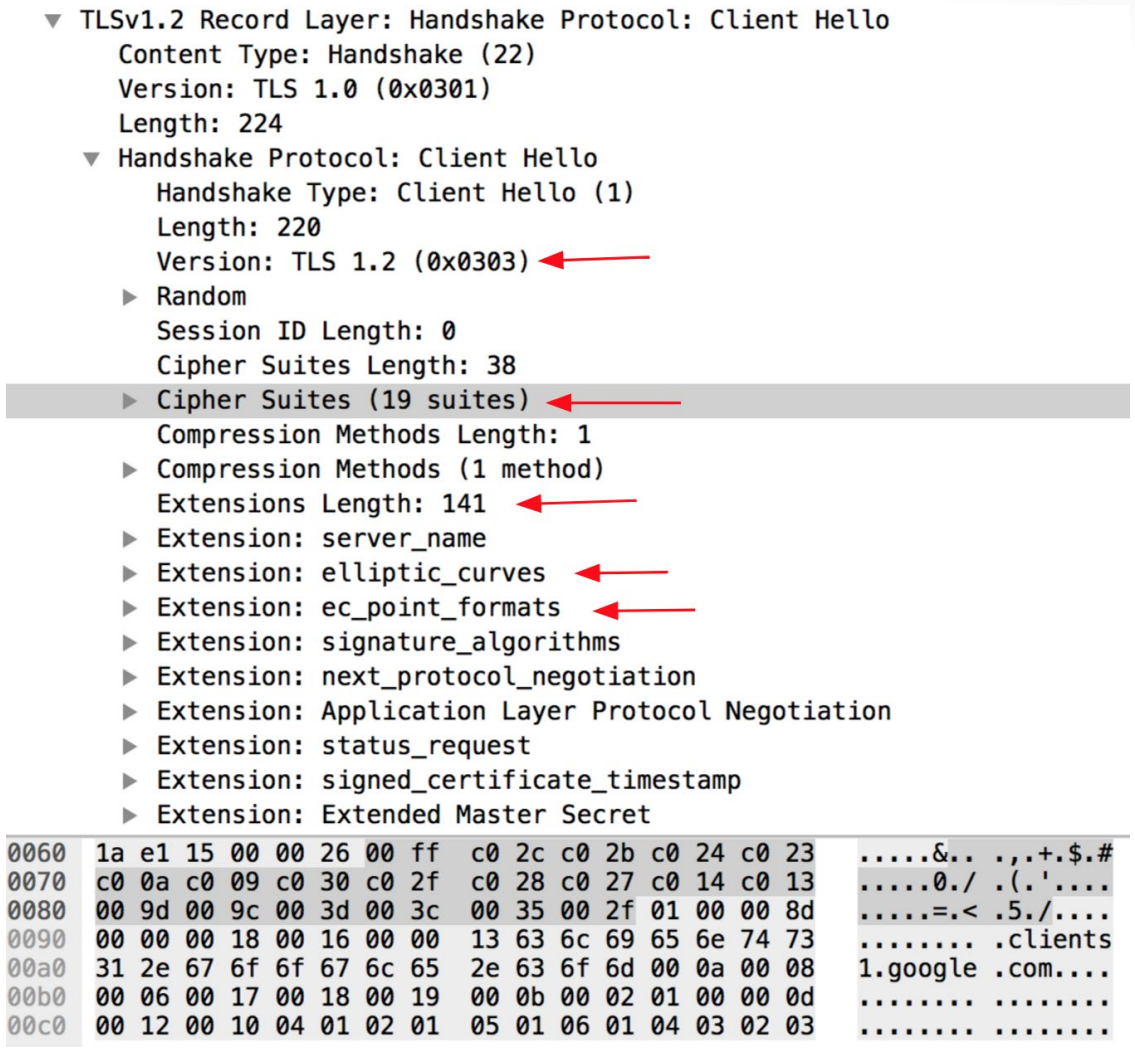
Page-Load Fingerprints

95.7% effective!



Patil, Borisov, "What can you learn from an IP?"
https://irtf.org/anrw/2019/anrw2019-final44-acmpaginated.pdf

TLS Fingerprinting Overview: JA3 and JA3S



- Hash of concatenated fields in the Client Hello message
- Unique fingerprints based on the TLS library and options
- JA3+JA3S for stronger application identification

JA3 TLS Client Fingerprint
ada70206e40642a3e4461f35503241d5

Source:
https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967

TLS Fingerprinting: False Positives and Evasion

Caution!

The JA3 fingerprints below have been collected by analysing more than 25,000,000 PCAPs generated by malware samples. These fingerprints have **not been tested against known good traffic yet and may cause a significant amount of FPs!**

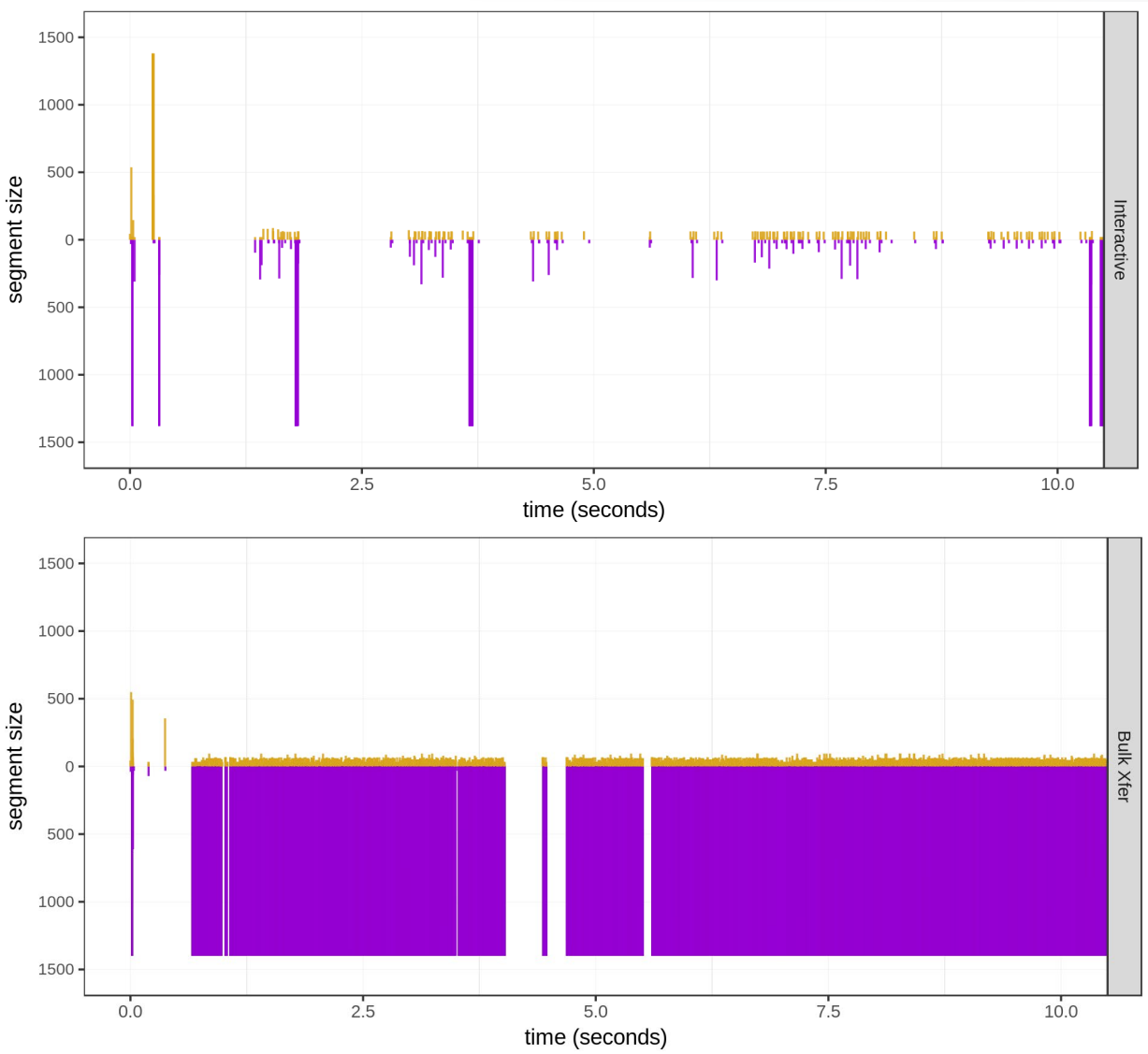
False Positives: 25%+ of blacklisted JA3s found to correspond to various versions of Chrome, Firefox, and IE11

Evasion: fairly trivial for sophisticated attackers

Cipher Stunting: randomized signatures

Source:
https://blogs.akamai.com/sitr/2019/05/bots-tampering-with-tls-to-avoid-detection.html

Traffic Analysis Overview

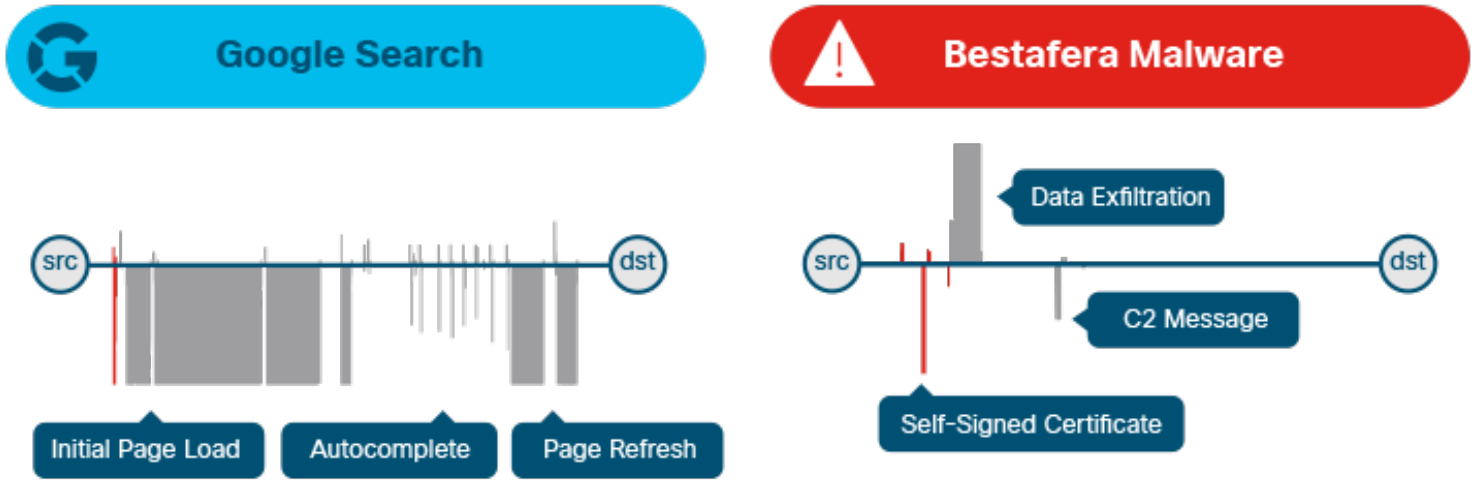


- Analyze packet lengths, interarrival times, TCP turn timing, entropy, etc.
- Track data flow
- Detect interactivity
- Identify encryption

Cisco Encrypted Traffic Analysis

- Initial Data Packet (IDP)
- Sequence of Packet Lengths and Times (SPLT)
- Byte distribution
- “TLS-specific features”

70% of malware will use some type of encryption



Source: https://blogs.cisco.com/security/detecting-encrypted-malware-traffic-without-decryption

Network Detection: Better with Plaintext

Serverside

- Web application vulns & attacks
- Injection attacks (e.g. SQLi, command injection)
- Desync attacks
- Data exfiltration
- Brute-force login attacks

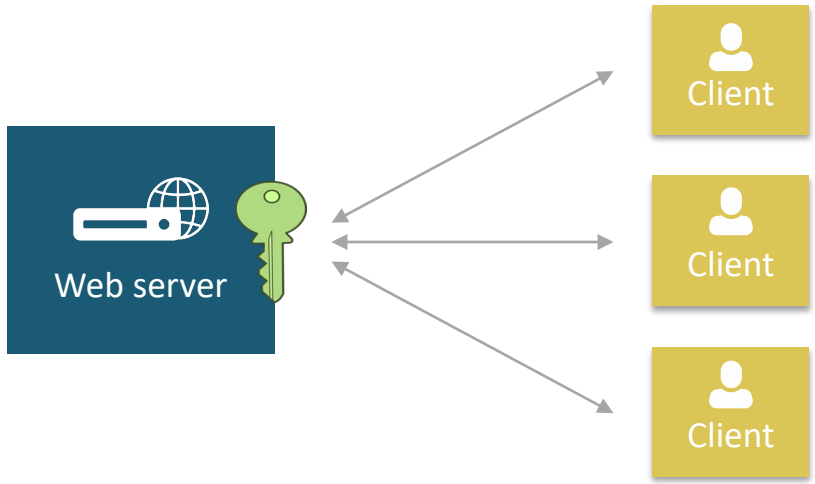
Clientside

- Threat intelligence
- DLP & exfiltration
- File scanning / carving
- Forensics
- Command & Control / Beaconing / Botnets

Perfect Forward Secrecy Overview

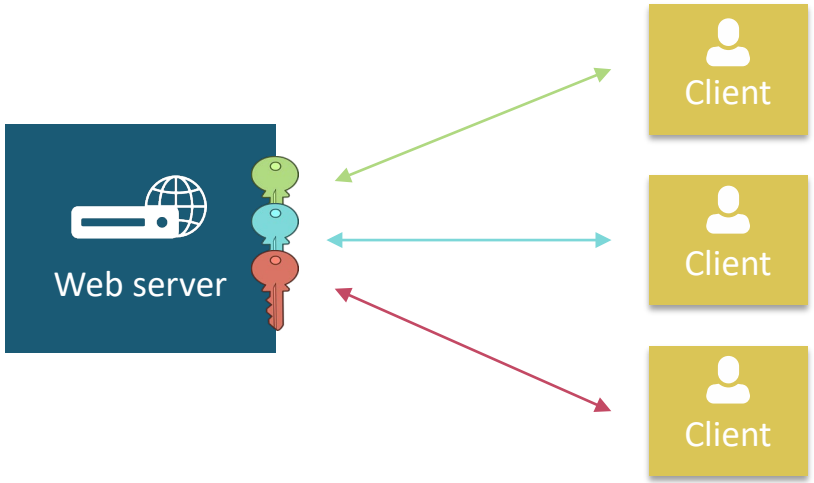
RSA Key Exchange

Long-term private key



Perfect Forward Secrecy

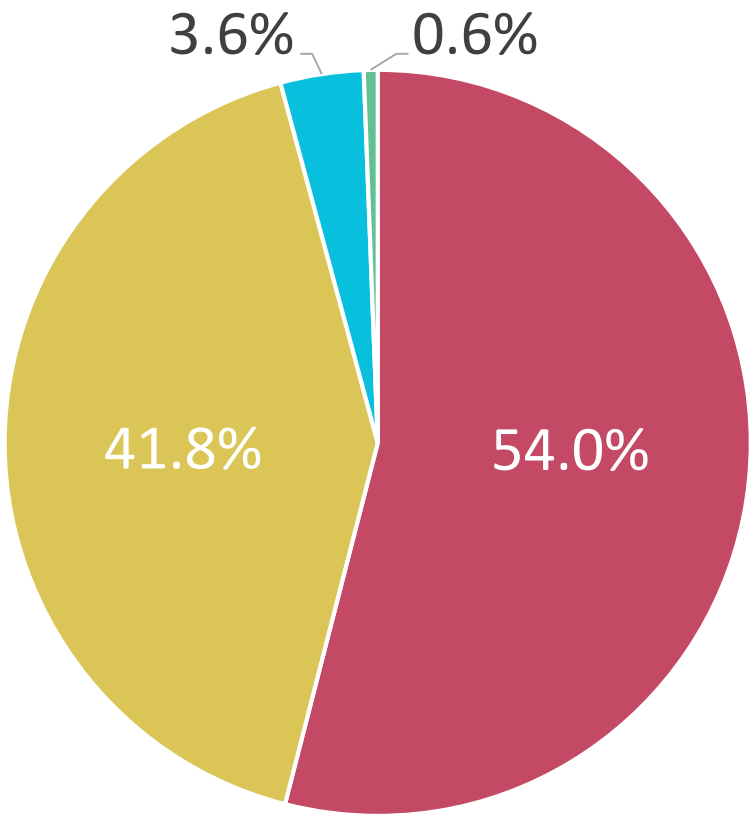
Unique ephemeral key per session



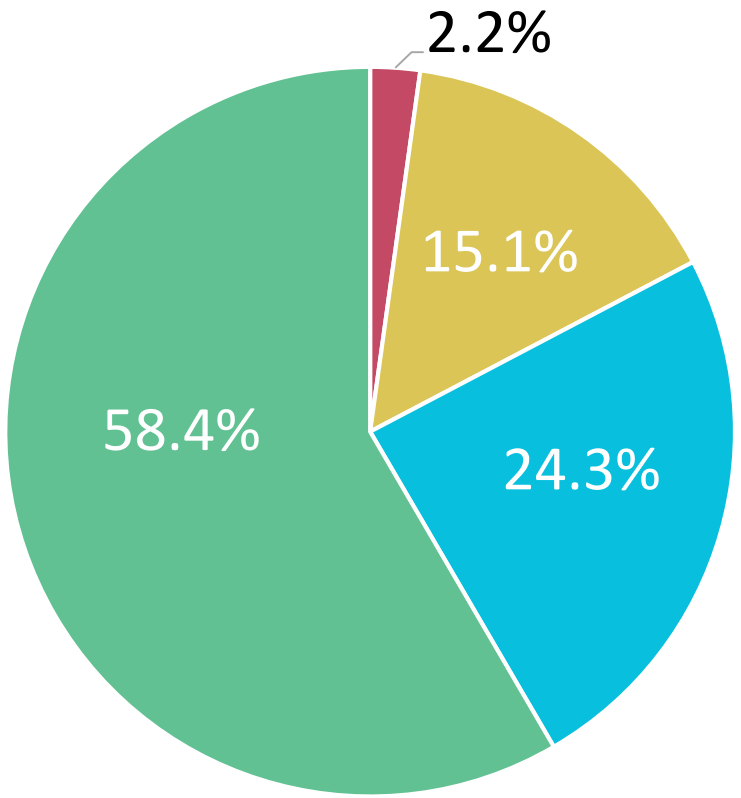
Session keys are ephemeral and *cannot* be derived from the private key.

Data remains secure even if the long-term private key is compromised.

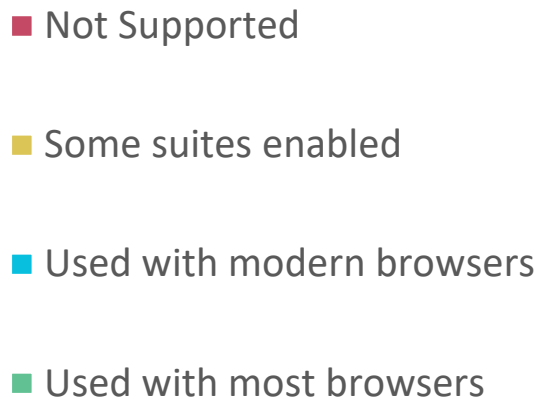
PFS Adoption: 2013 – 2020



Trustworthy Internet Movement SSL Pulse
October 2013

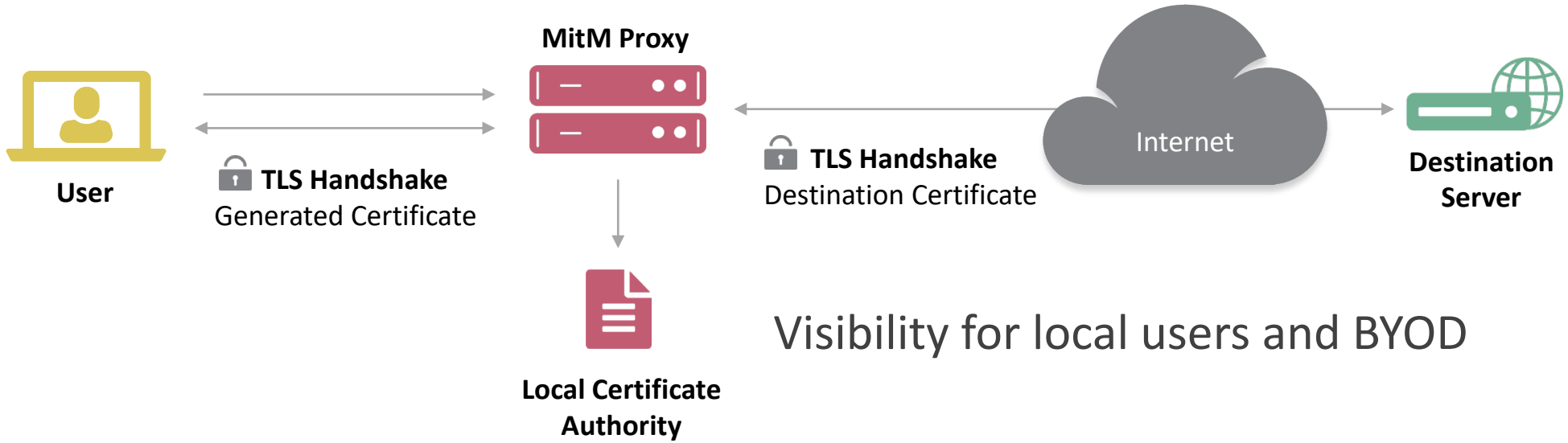


Trustworthy Internet Movement SSL Pulse
January 2020



SSL/TLS Interception: "Break-and-Inspect"

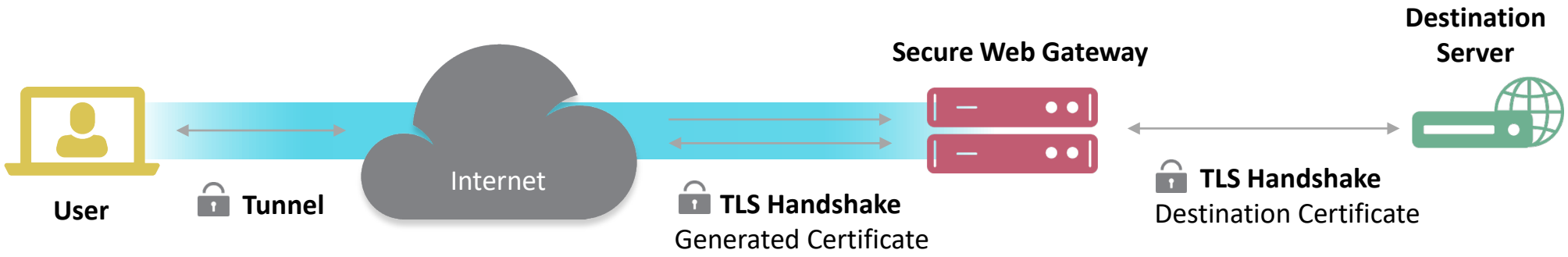
- Requires a local CA
- No public key pinning or certificate transparency
- No client certs or mutual TLS
- Limited support for certificate status or revocation
- Potential for weak keys, incorrect certificate validation, and vulnerabilities



Visibility for local users and BYOD

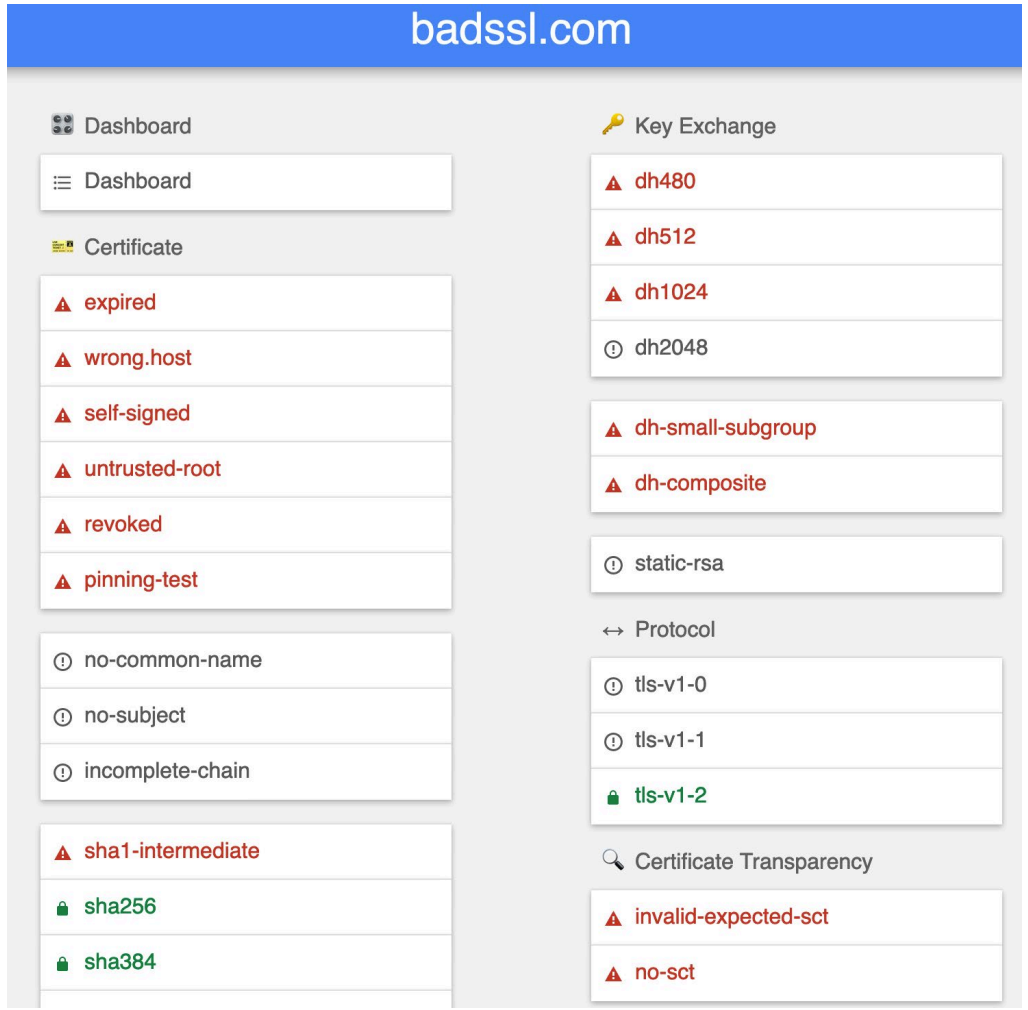
SSL/TLS Interception: Secure Access Service Edge (SASE)

- Same SSL/TLS interception challenges and benefits
- Source IP is obscured
- Tunnel established by client VPN or Internet Gateway
- No option for decrypted feed or key logging for analysis (yet)



SWG service performs URL filtering and content inspection

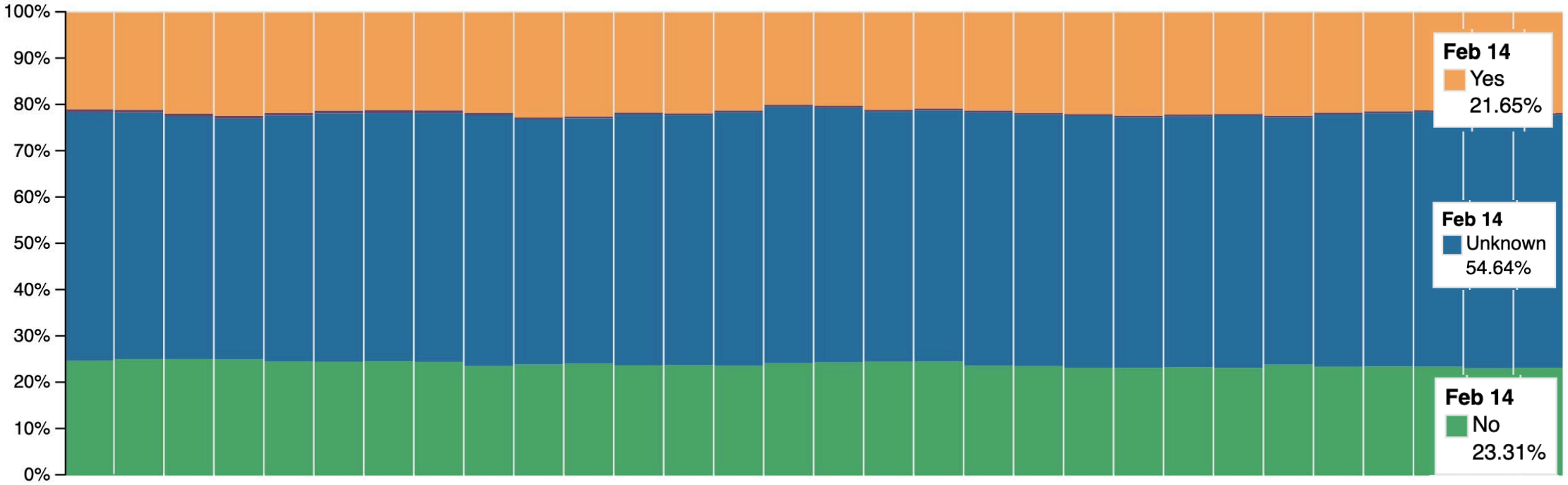
SSL/TLS Interception: Potential Weaknesses



Test for weaknesses with badssl.com

SSL/TLS Interception: Trend

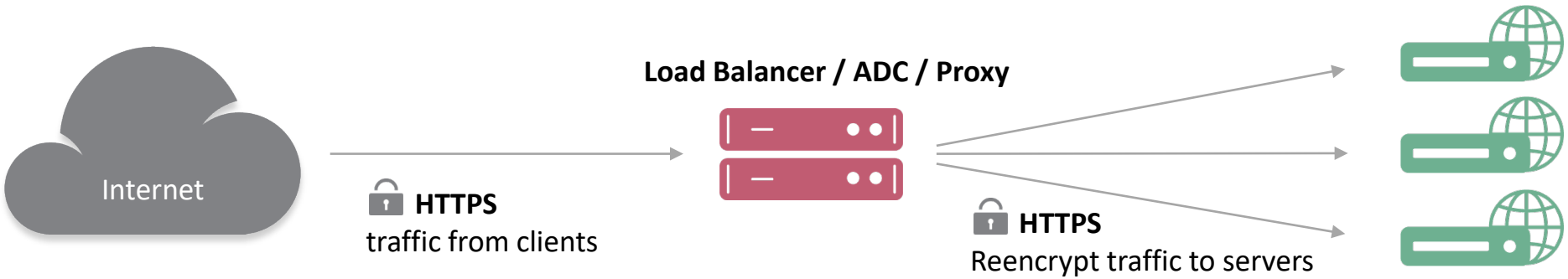
20%+ of HTTPS connections observed over the past 30 days have been intercepted!



Source:
https://malcolm.cloudflare.com/

SSL/TLS Termination & Re-encryption

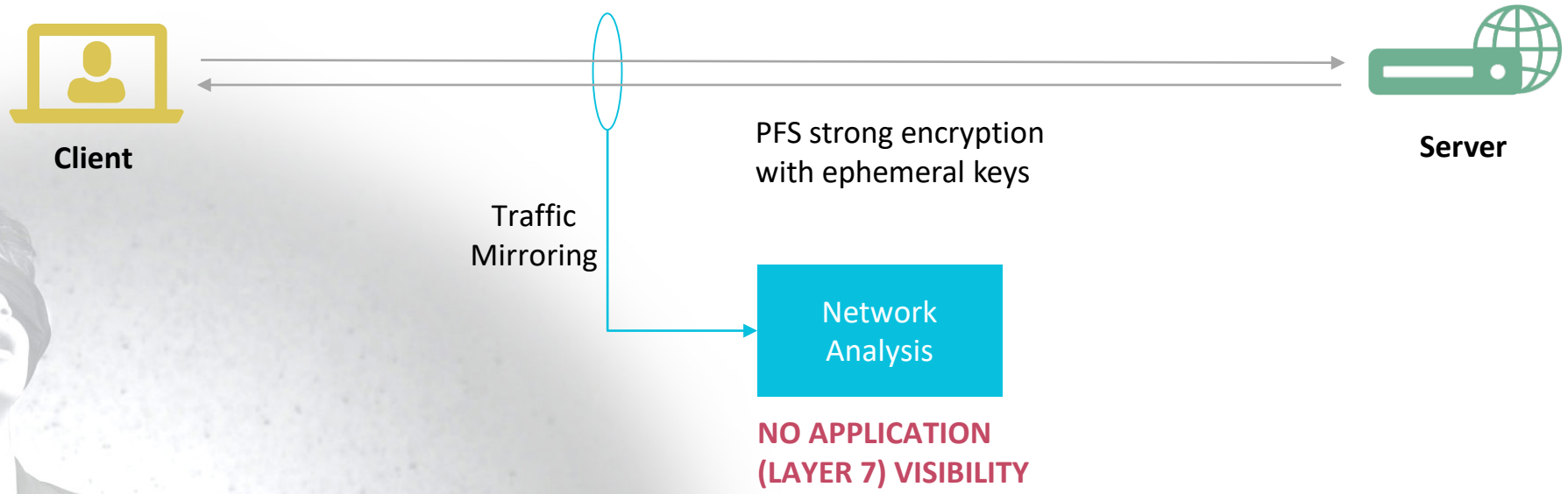
- Enable load balancing, content switching, and optimization
- Minimize SSL/TLS handshakes through connection reuse
- Centralize certificate management and authentication



Visibility for local services

Out-of-band Analysis & Forensics

PFS breaks out-of-band network analysis and packet capture that needs to perform decryption for analysis

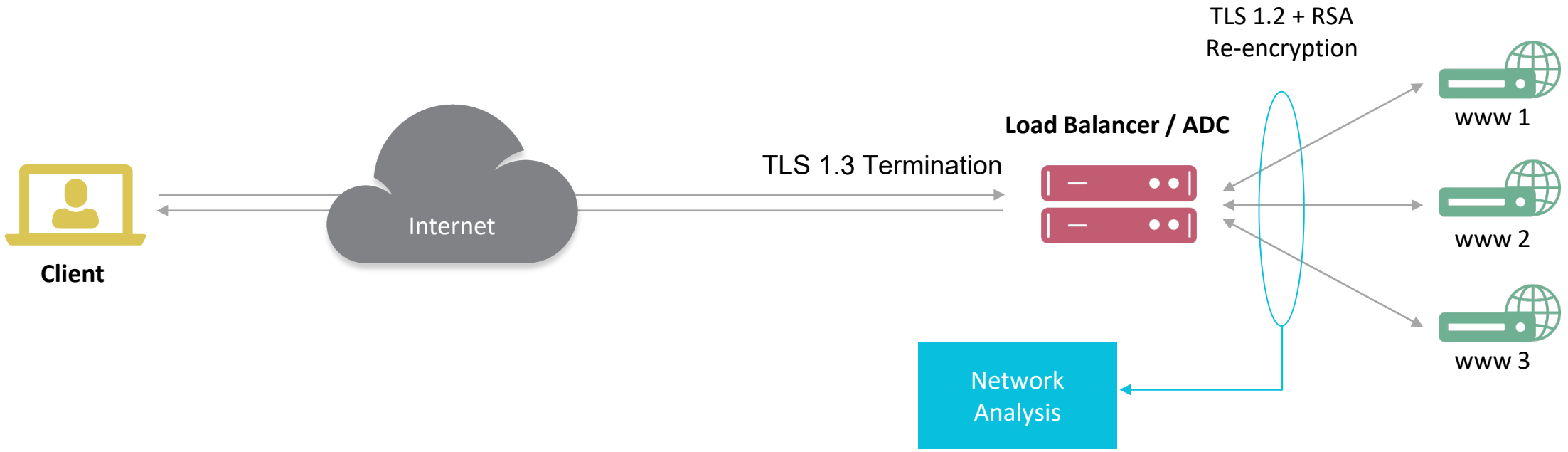


NO APPLICATION (LAYER 7) VISIBILITY

Perfect Forward Secrecy breaks DLP, IDS/IPS, malware detection, PCAP analysis, AANPM, etc.

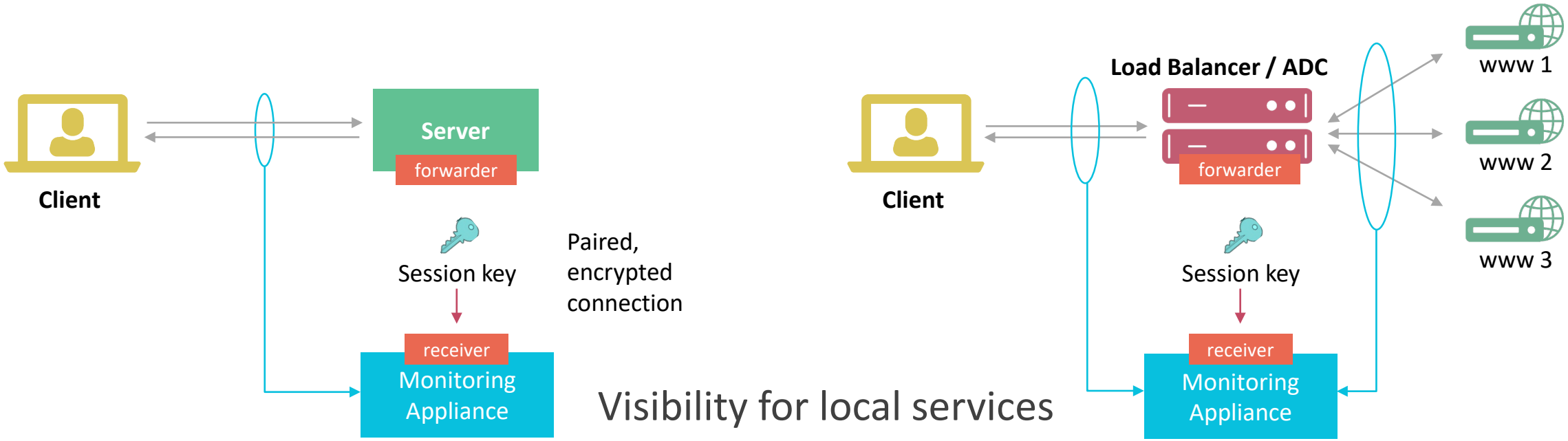
Out-of-band Analysis: TLS Downgrade

- Reencrypt internal connections with TLS 1.2 + RSA
- Limited visibility to client-side traffic
- Temporary solution until TLS 1.2 is phased out



Out-of-band Analysis: Session Key Forwarding

- Maintains the integrity of end-to-end encryption
- Out-of-band solution using port mirror or network tap
- Analysis of the real packets



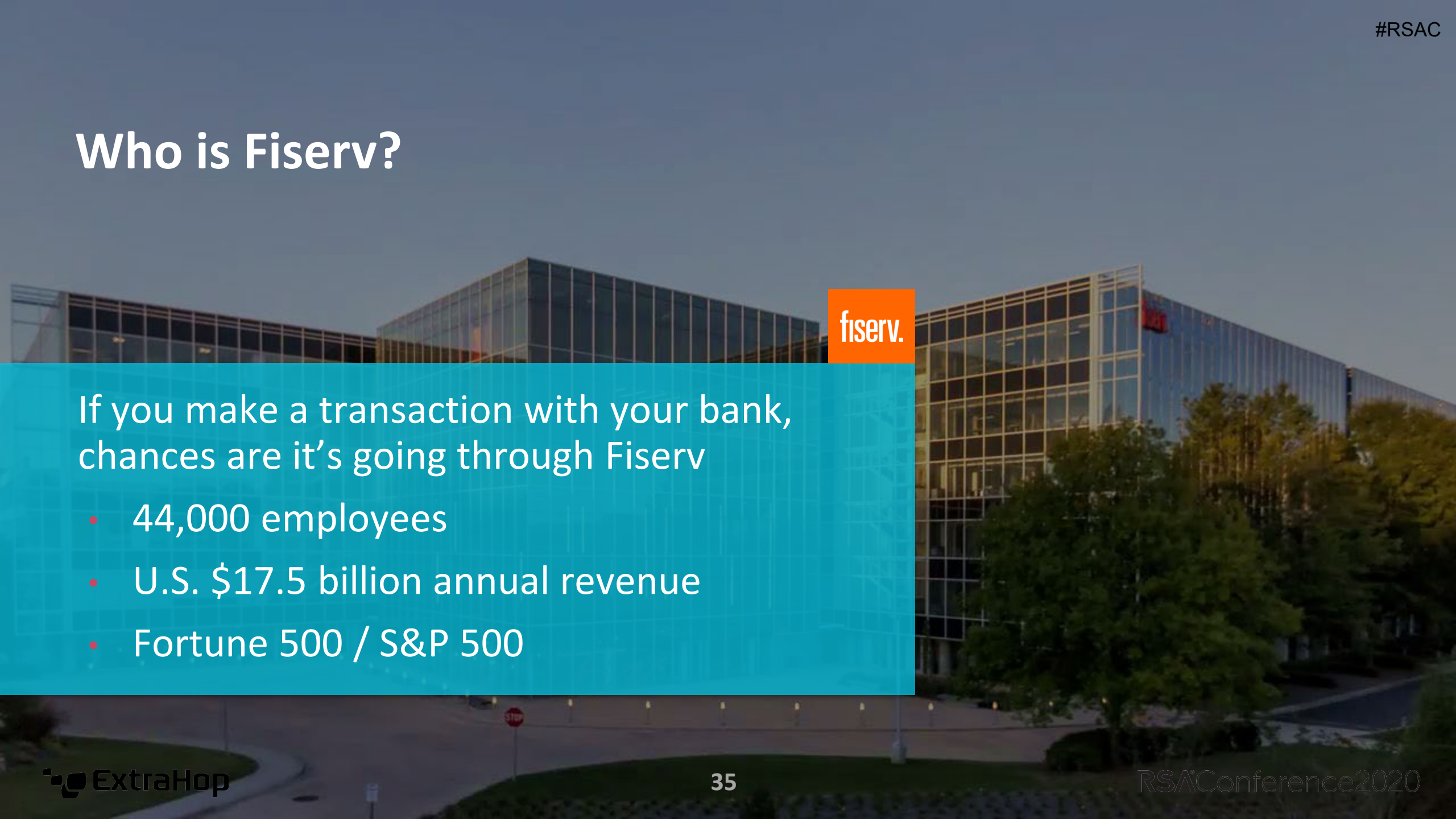
Recommended Next Steps

- Disable DoH
  - Configure enterprise policy and Firefox canary domain
- Use SSL/TLS interception for user / BYOD traffic
  - Test security impact with badssl.com
  - Request key logging from your vendor to enable additional analysis
- Use session-key forwarding for local services
  - Deploy key forwarders for ADCs, proxies, and OS-level crypto providers

RSAConference2020

Real-Time Analysis and Decryption at Scale

Who is Fiserv?



If you make a transaction with your bank, chances are it's going through Fiserv

- 44,000 employees
- U.S. $17.5 billion annual revenue
- Fortune 500 / S&P 500

Decrypting PFS at Fiserv

What does decryption give us?

- User authentication auditing
- Attack surface hardening (enumeration attacks, what APIs are accessed from where)
- General availability improvements (CIA triad)

Decrypting PFS at Fiserv

Why Perfect Forward Secrecy?

- Newer standards protect sensitive consumer information
- We encrypt traffic deeper in the infrastructure
- We ask third-party vendors to use stronger encryption

Decrypting PFS at Fiserv

Worked with ExtraHop to develop a solution for decrypting PFS

3,000

session-forwarding agents deployed in infrastructure across several datacenters

6K PFS

sessions per second

HTTPS

and more

Ongoing

and growing effort

- Deployed via automation today
- Moving into CI/CD workflows

Apply / Next Steps

WE AS AN INDUSTRY NEED TO PREPARE

Who is still using outdated standards (SSLv3)?

Legacy systems

TLS 1.3 (AND ENCRYPTION IN GENERAL) IS NOT A SILVER BULLET

Confidentiality and integrity

But as previously discussed, you can't secure what you can't see

VISIBILITY INTO THIRD-PARTY SERVICES

Logging is a slow follower to need

3rd party connections are the least logged connections

With wire data you can see what data is going to which third-parties (CCPA and GDPR)

RSAConference2020

Questions?