

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: PART3-W09

HTTPS: Why Privacy Doesn't Equal Security

Hal Lonas

SVP & CTO, SMB and Consumer
OpenText

David Dufour

VP Cybersecurity & Engineering
OpenText



Who are these guys?

HAL LONAS

SVP and CTO



SUPERPOWERS

- Ultimate frisbee
- Machine learning /AI
- Cybersecurity since 2000

DAVID DUFOUR

VP Engineering & Cybersecurity



SUPERPOWERS

- Skateboarding
- Cybersecurity

Get Set Up With Polling

Session ID: PART3-W09



The image displays three sequential screenshots of a mobile application interface for a conference session:

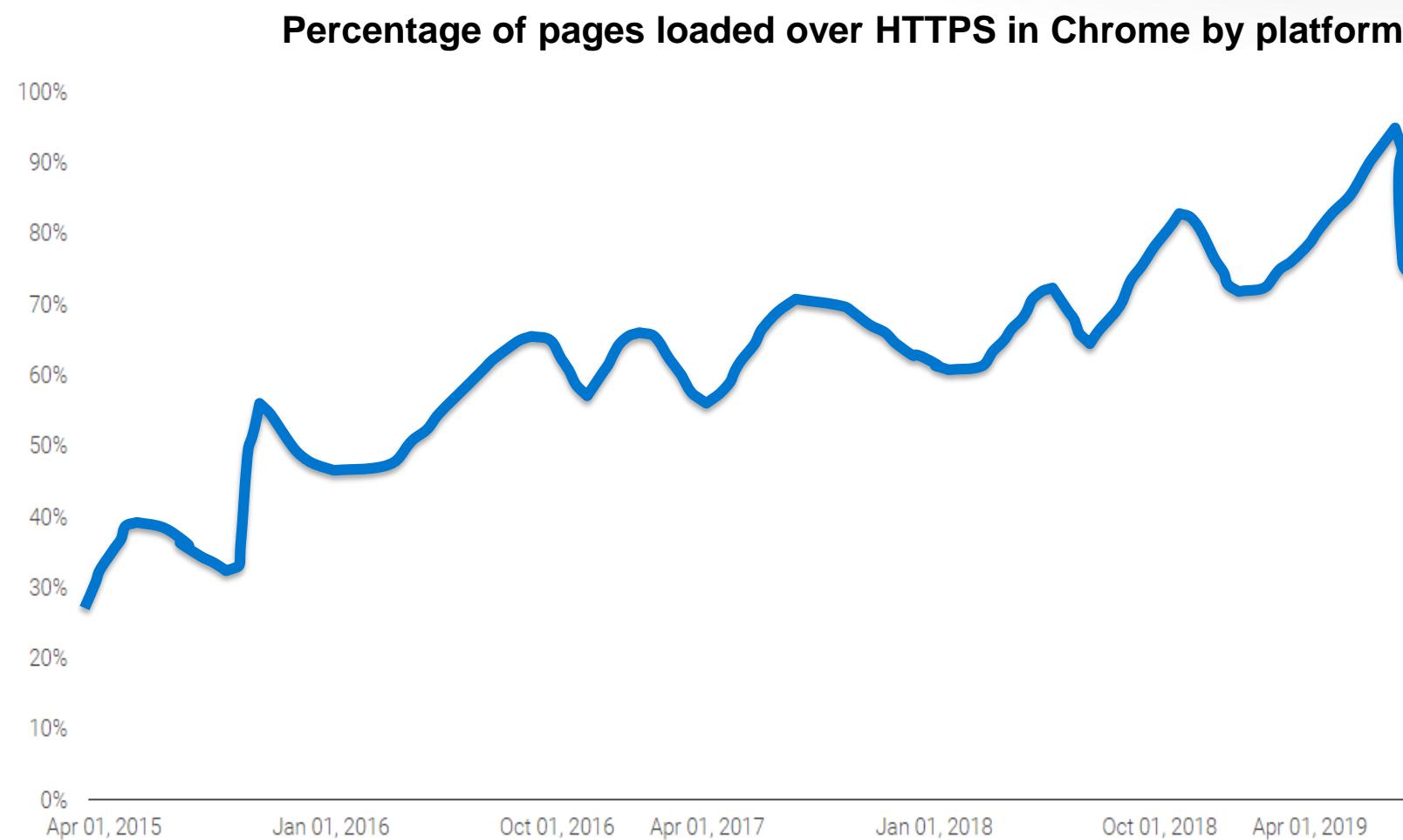
- Screenshot 1:** Shows the session details for "ACB-F01 The Modus Operandi of EV Certificates Fraudsters: Findings from the Field". It includes the date (28 Feb), time (8:30 AM - 9:20 AM), and location (Moscone West 3024). A yellow arrow points to the "MARK AS FAVORITE" button.
- Screenshot 2:** Shows the session details with the "OPEN" button highlighted. Below it, a poll titled "Did you enjoy RSAC US19 Conference?" is displayed, showing 0 votes and a 15-hour remaining time.
- Screenshot 3:** Shows the poll results for the same question. It includes two radio buttons: "Yes" and "No", both of which are unselected. A blue "SUBMIT" button is at the bottom.

POLL: Users spend what percentage of their time on HTTPS pages?

- 22%
- 57%
- 90%
- 100%

<https://rsa1-live.eventbase.com/polls?event=rsa2020&session=1190795663>

The growth of HTTPS adoption



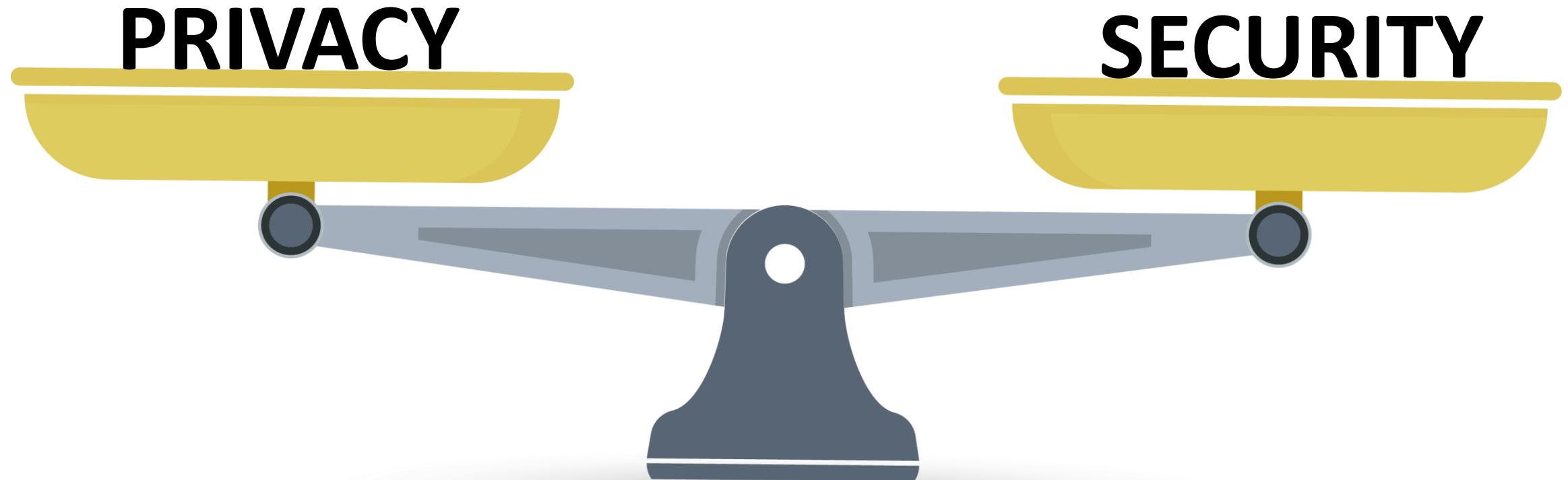
Desktop users load **more than half** of the pages they view over HTTPS and spend **close to 90 percent** of their time on HTTPS pages.

<https://transparencyreport.google.com/https/overview?hl=en>

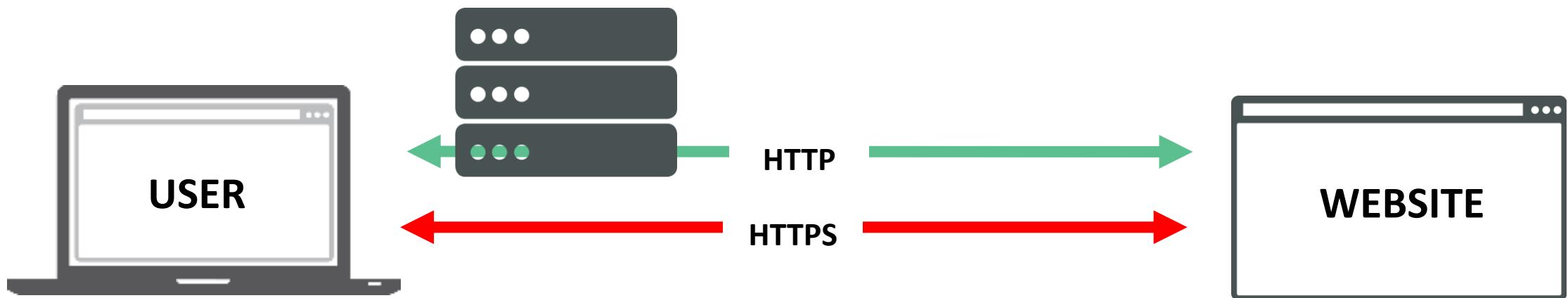
Of the phishing and malware domains Webroot identified to be active in July of 2019, **54%** of them were listening on port 443.

F5 Labs "2019 Phishing and Fraud Report"

Let's discuss the privacy vs. security debate

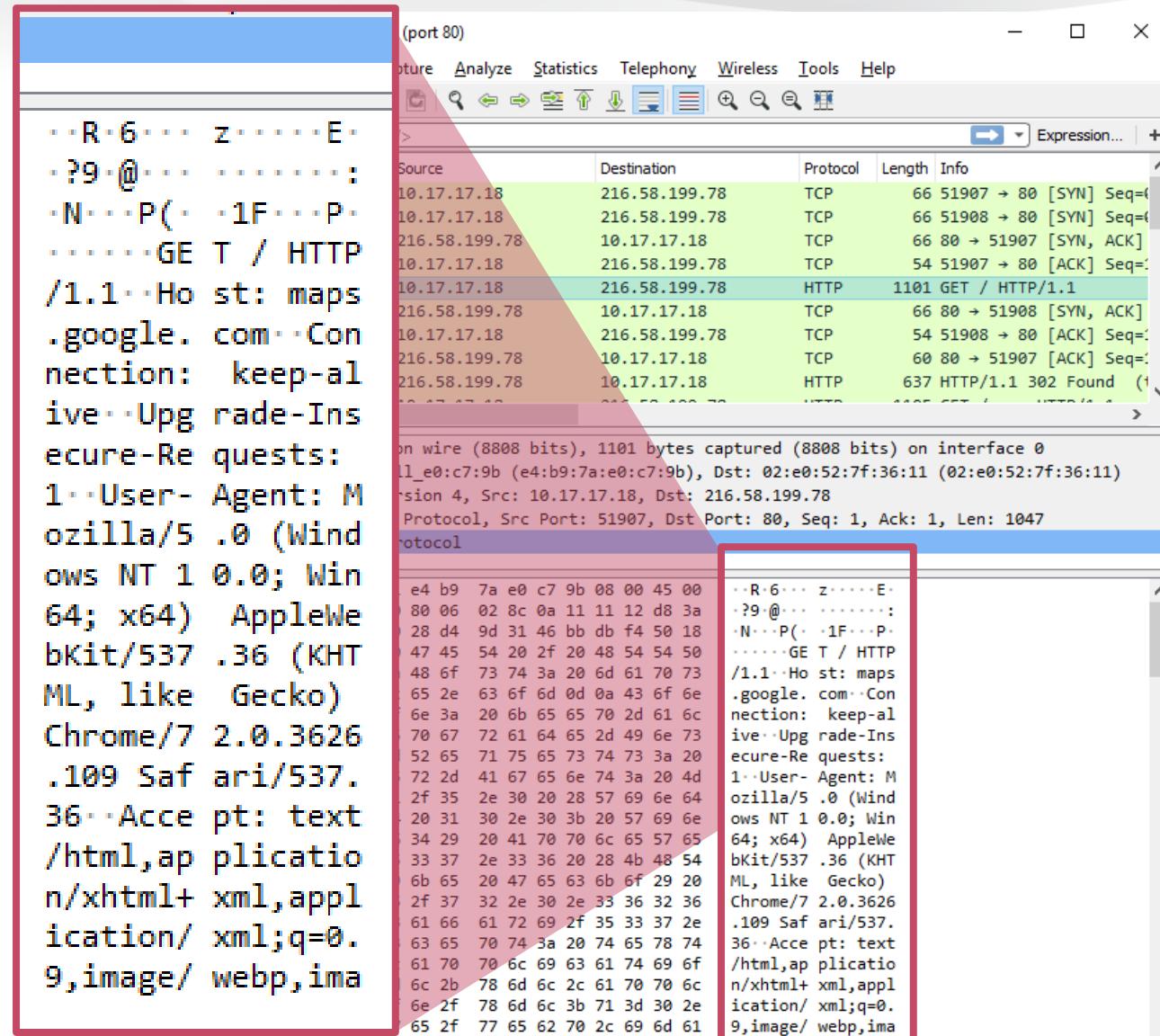


Architecture

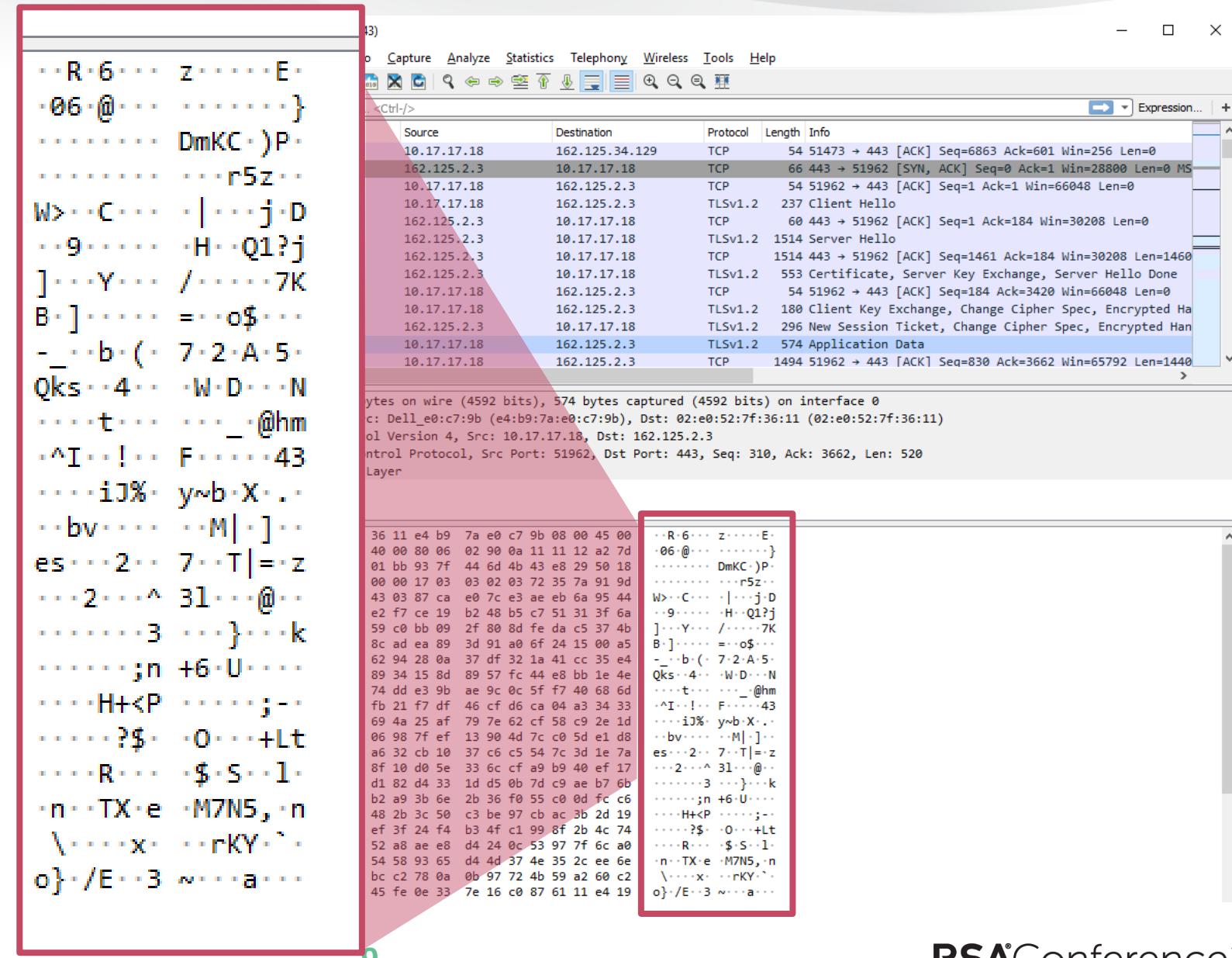


Don't have full visibility with HTTPS

HTTP vs. HTTPS



HTTP vs. HTTPS



Does every website need to be HTTPS?

The screenshot shows the Wells Fargo homepage. At the top, there's a navigation bar with links for Flying, Fake News, GCC issues, HTTPS, RSA links, ML topics, Webroot Cybersecu..., 2018 Phishing and..., and TurboTax® Tax Pre... . Below the navigation bar is the Wells Fargo logo and a red banner with links for Enroll, Customer Service, ATMs/Locations, Español, and Search. The main menu includes Personal, Small Business, Commercial, Financial Education, and About Wells Fargo. Below the menu, there are links for Banking and Credit Cards, Loans and Credit, Investing and Retirement, Wealth Management, and Rewards and Benefits. On the left, there's a login form for "View Your Accounts" with fields for Username and Password, and a "Save username" checkbox. A "Sign On" button is at the bottom of the form. The main content area features a large image of a father carrying a young child on his shoulders, with the text "Member FDIC" and "Simplified banking". It also includes a subtext about Everyday Checking being convenient and fast, and a "Start Now >" button.

wellsfargo.com

Flying | Fake News | GCC issues | HTTPS | RSA links | ML topics | Webroot Cybersecu... | 2018 Phishing and... | TurboTax® Tax Pre...

WELLS FARGO

Enroll | Customer Service | ATMs/Locations | Español | Search

Personal Small Business Commercial Financial Education About Wells Fargo

Banking and Credit Cards | Loans and Credit | Investing and Retirement | Wealth Management | Rewards and Benefits

View Your Accounts

Username
Password
 Save username

Sign On

Member FDIC

Simplified banking

Everyday Checking provides convenience and fast access. Open in minutes.

Start Now >

Does every website need to be HTTPS?

The screenshot shows the Us Weekly website. At the top, there's a navigation bar with categories: News, Stylish, Entertainment, Royals, Moms, Food, Pets, Podcasts, Video, and More. A "Subscribe Now" button is also visible. Below the navigation, there's a "Latest News" section featuring a photo of three people and a "Food" article about Khloe Kardashian, Shay Mitchell, and others getting in-home bars. Another section shows photos of Bachelor Peter and his exes, with an "EXCLUSIVE" tag and a headline about Victoria F. The right side features a "PERFORMIX" advertisement for SST H2, which promises to supercharge energy, focus, and metabolism.

News Stylish Entertainment Royals Moms Food Pets Podcasts Video More ▾

Subscribe Now

Latest News

FOOD

Drink Up! Khloe Kardashian, Shay Mitchell, More Stars With In-Home Bars

OMG

Orlando Bloom Got a Tattoo in Honor of Son

TOP HEADLINES

EXCLUSIVE

Bachelor Peter's Ex Reveals How She Knows 'Self-Centered' Victoria F.

PERFORMIX

SUPERCHARGE YOUR ENERGY, FOCUS, AND METABOLISM

FUEL YOUR PURPOSE WITH SST H2

Does every website need to be HTTPS?



Not secure

nhultimate.com/cms/index.php

The screenshot shows a web browser displaying the URL <http://nhultimate.com/cms/index.php>. The page title is "NH ULTIMATE.COM". A red box highlights the login form, which contains fields for "Username" (containing "hal@lona...") and "Password" (containing a series of dots). Both fields have small message bubble icons with the number "1" next to them, indicating new notifications. Above the login form, there is a navigation bar with links: "mate-Pickup", "Mira-Mesa-Pickup", "nel-Valley-Pickup", and "Seacoast-Disc-Golf". Below the navigation bar, there is a button labeled "Font Style" and another labeled "Text Size". A message at the bottom of the page says "PLEASE START A GAME, OR UPDATE STATUS." and "this year".

POLL: If you were forced to pick, what is most important to you and your organization?

- Privacy
- Security

<https://rsa1-live.eventbase.com/polls?event=rsa2020&session=1190795663>



The Problems HTTPS Creates

POLL: What percentage of malicious sites are found on benign domains?

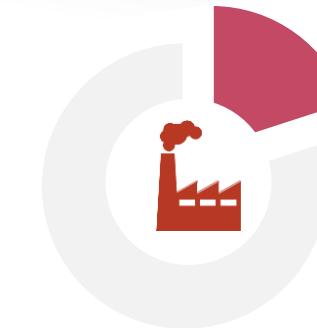
- 2%
- 24%
- 64%
- 82%

<https://rsa1-live.eventbase.com/polls?event=rsa2020&session=1190795663>

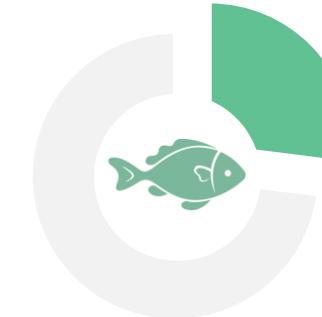
The HTTPS Security and Policy Gap



**1 in 4 (24%) malicious URLs is hosted
on an otherwise non-malicious sites**



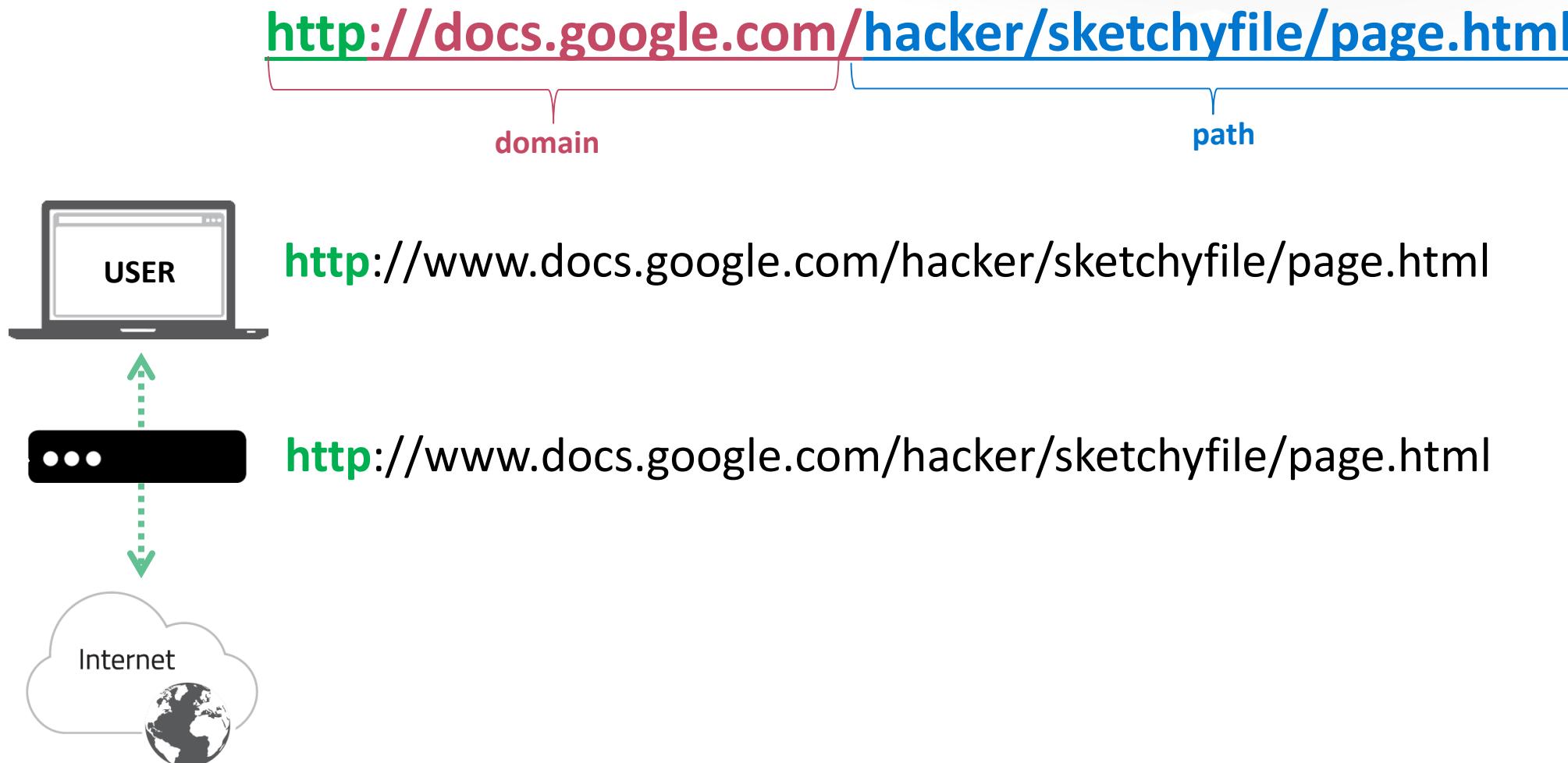
**20% Non-malicious
sites hosting bad
URL: Manufacturing**



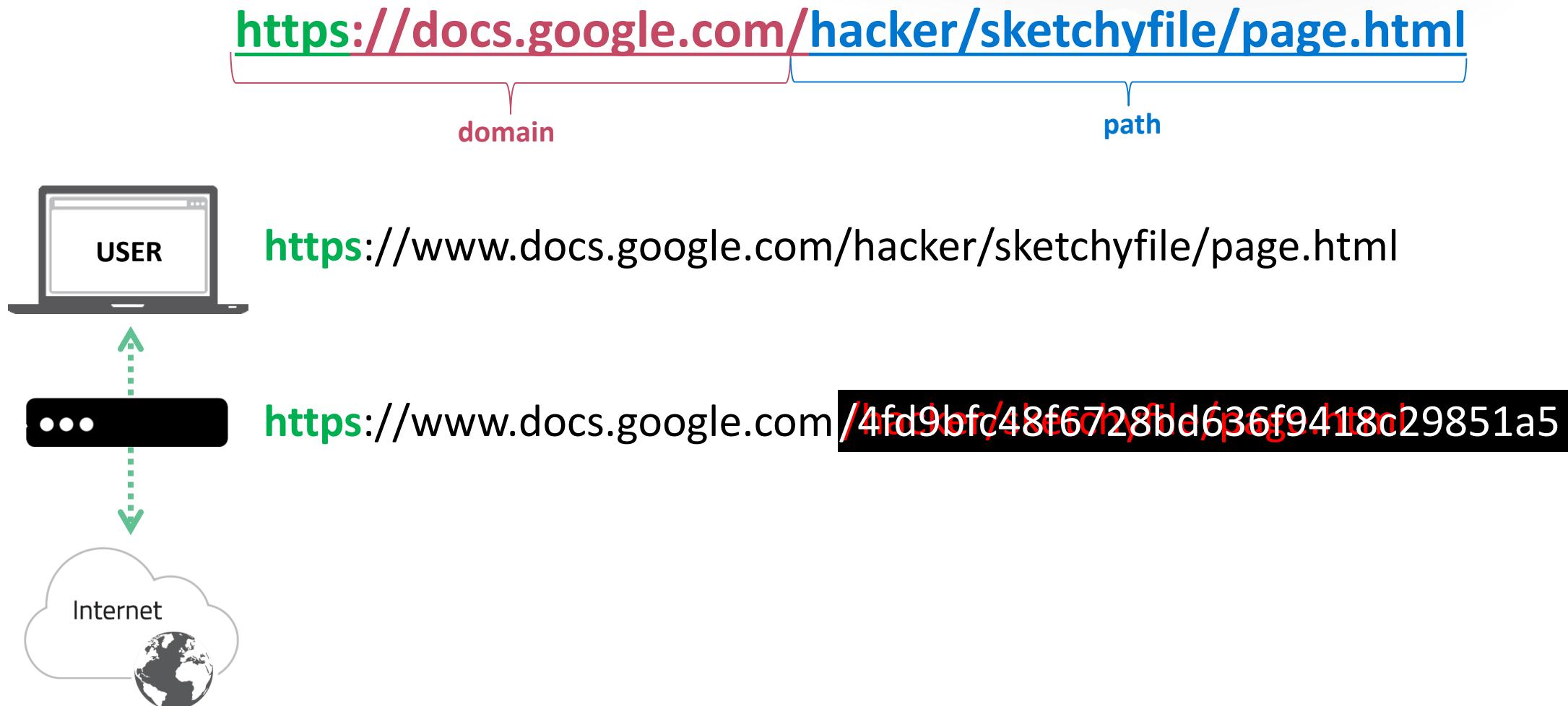
**27% of phishing sites used
HTTPS to trick users into
thinking the site was safe**

Based on Webroot URL categorization data from January to November 2019.

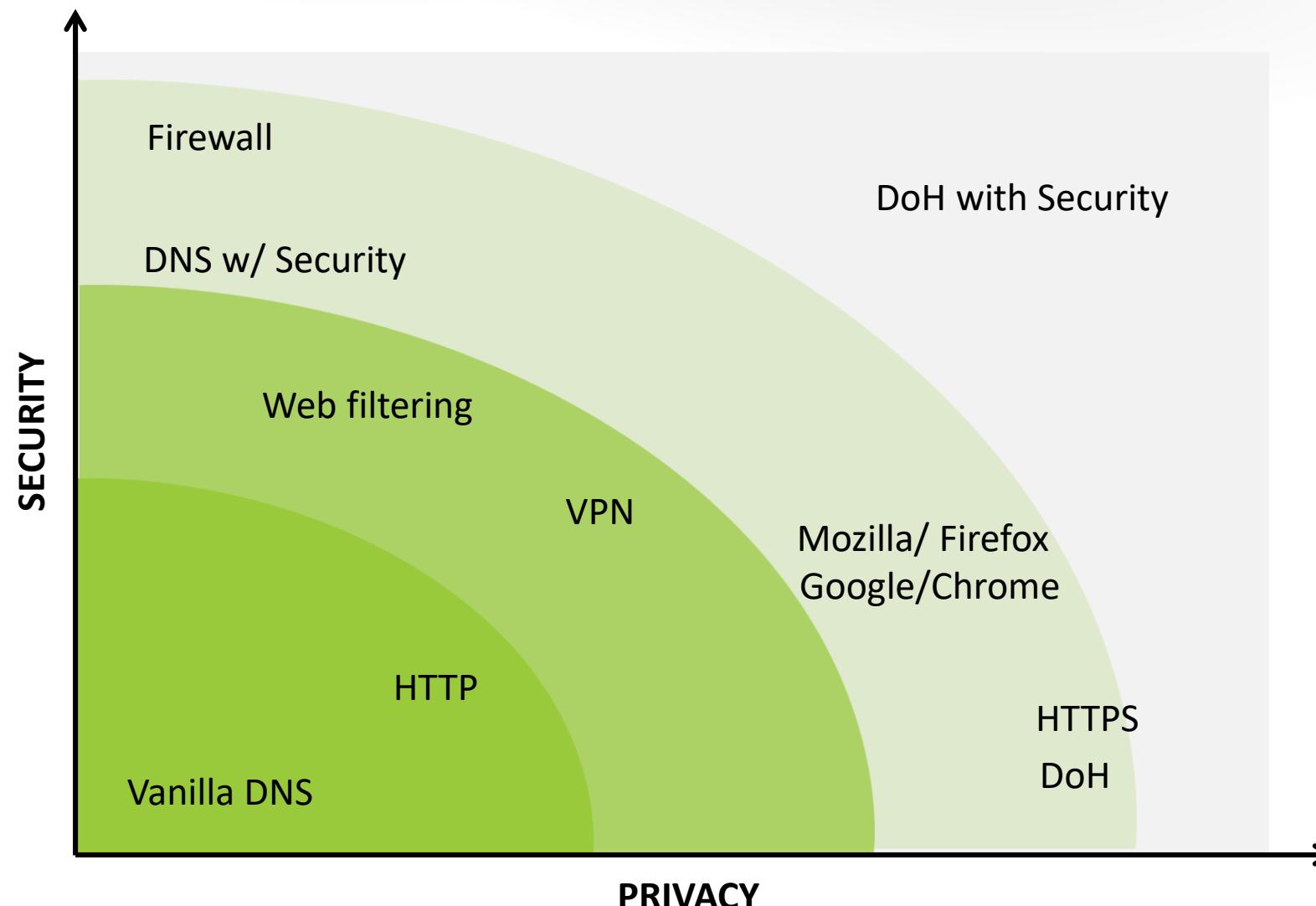
Privacy vs. Security: What does it mean for network devices?



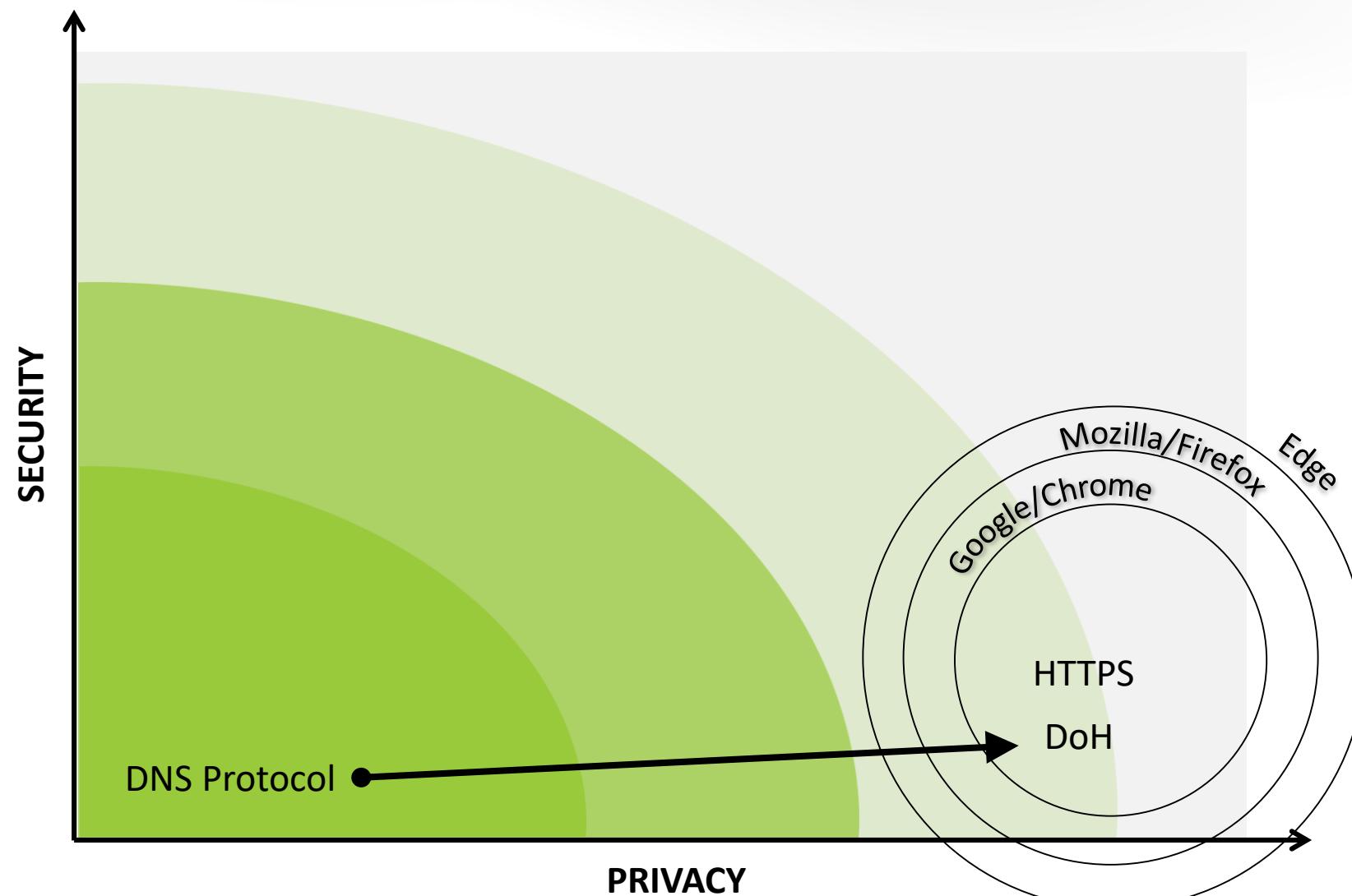
Privacy vs. Security: What does it mean for network devices?



Spectrum of choices



When DNS meets HTTPS



Godlua – The first malware to leverage DoH

Godlua, a Linux DDoS bot, is the first-ever malware strain seen using DoH to hide its DNS traffic.



```
strcpy(v9, "https://api.github.com/repos/helegedada/heihei");
v0 = (void *)http_init(1);
http_set_headers(
    v0,
    "User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0;+http:
v1 = http_get((int)v0, v9);
if ( v1 && *(_DWORD *)(v1 + 16) )
{
    v2 = strstr(*(const char **)(v1 + 20), "\"description\":\"");
    v3 = (int)(v2 + 15);
    v4 = strstr(v2, "\",\"");
    *v4 = 0;
    v5 = "d.heheda.tk";
    if ( v4 != (char *)v3 )
        v5 = (const char *)v3;
    v6 = gethostbyname(v5);
    if ( v6 )
        v7 = **(_DWORD **)v6->h_addr_list;
    else
        v7 = 0;
    ccip = v7;
    env = 0;
    ccport = 0x22FF;
```



Cybercriminals & HTTPS

POLL: Did your last malware attack come over HTTPS?

- Yes
- No
- I don't know

<https://rsa1-live.eventbase.com/polls?event=rsa2020&session=1190795663>

What are the ingredients to make the bomb?

PayPal
Verify Account
Please complete the form below to verify your Profile information and restore your account access.

Personal Information
Make sure you enter the information accurately, and according to the formats required.
Fill in all the required fields.

*Email:	<input type="text"/>
*Password:	<input type="password"/>
*Re-type Password:	<input type="password"/>
*Full Name:	<input type="text"/>
*Date of Birth:	month <input type="text"/> day <input type="text"/> year <input type="text"/>
*Mother's Maiden Name:	<input type="text"/>
*Mobile Phone Number:	<input type="text"/>

This number will be used to contact you about Security Measures and/or other issues regarding your PayPal account.

Account Information
Enter card information as accurately as possible.
For card number, enter numbers only please, no dashes or spaces.

*Account Number:	<input type="text"/>
*Sort Code:	<input type="text"/>
*Card Number:	<input type="text"/>
*Expiration Date:	month <input type="text"/> year <input type="text"/>
*Card Verification Number:	<input type="text"/> Help finding your Card Verification Number

Address
Enter your information as accurately as possible.

*Address:	<input type="text"/>
*City:	<input type="text"/>
*County:	<input type="text"/>
*Postcode:	<input type="text"/>

Required Field*
For your protection, we verify credit card information.
The process normally takes about 30 seconds, but it may take longer during certain times of the day. Please click Verify to update your information.

Copyright © 1999-2014 PayPal, Inc. All rights reserved.
PayPal Pty Limited ABN 93 111 195 389 (AFSL 304962). Any general financial product advice provided in this site has not taken into account your objectives, financial situations or needs.

[Verify](#)

Welcome to Google Docs. Upload and Share Your Documents Securely

Sign in with your email address to view or download attachment

Select your email provider

Gmail Sign in with Gmail

Email

Password

Sign in to view attachment

Stay signed in Need help?

Access your documents securely, no matter your location

g g g g g g g

Google Privacy & Terms Help

Bank of America

Sign In to Online Banking

Online ID [Minutes](#) Save this Online ID

Create Free SSL Certificate [Forgot your Passcode?](#)

Sign in

Secure area

Privacy & Security

Bank of America, N.A. Member FDIC. Equal Housing Lender [Equal Housing Lender](#)
© 2016 Bank of America Corporation.

Enjoy SSL Benefits

- Protect user data & gain trust
- Improve Search Engine Ranking
- Prevent forms of website hacking

2,000,000+ Free SSL Certificates Created

We put security certificates to the test



Score: 92

Score Summary

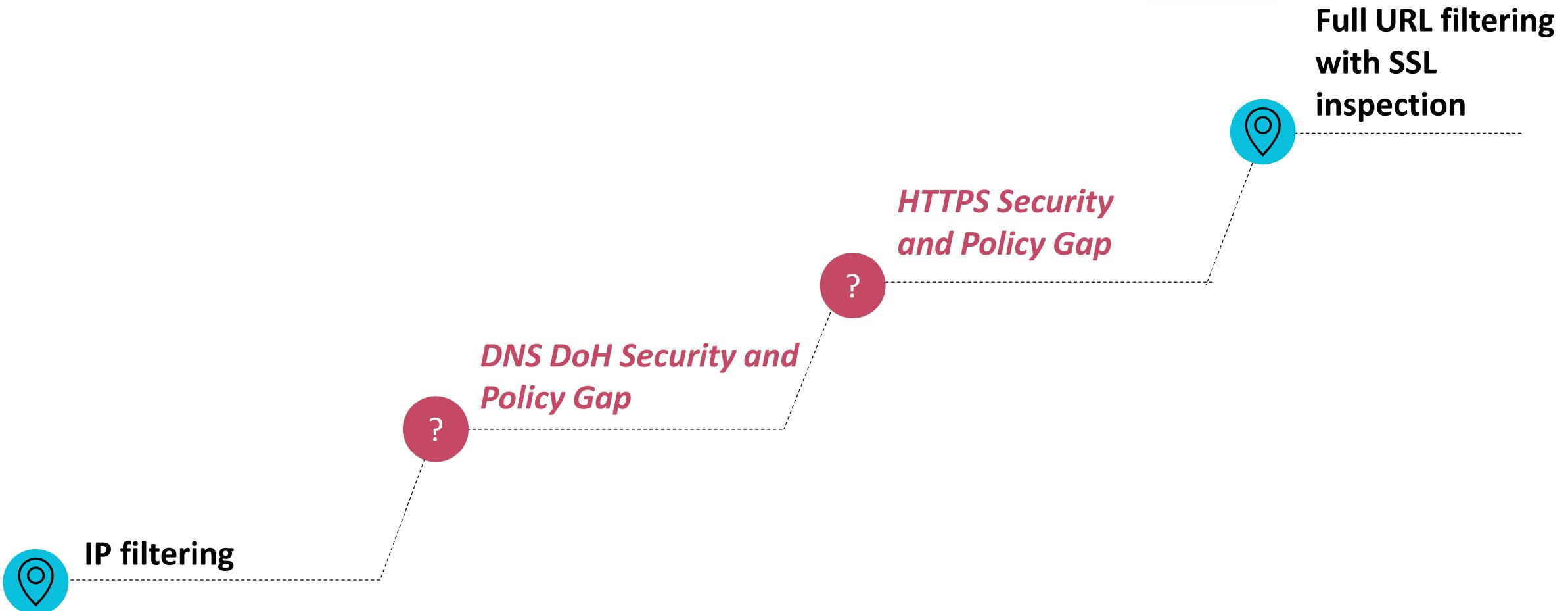
These are safe certificates that have not been tied to phishing. There is a very low predictive risk that your infrastructure and endpoints will be exposed to attack.

**HARVEY
MUDD
COLLEGE**

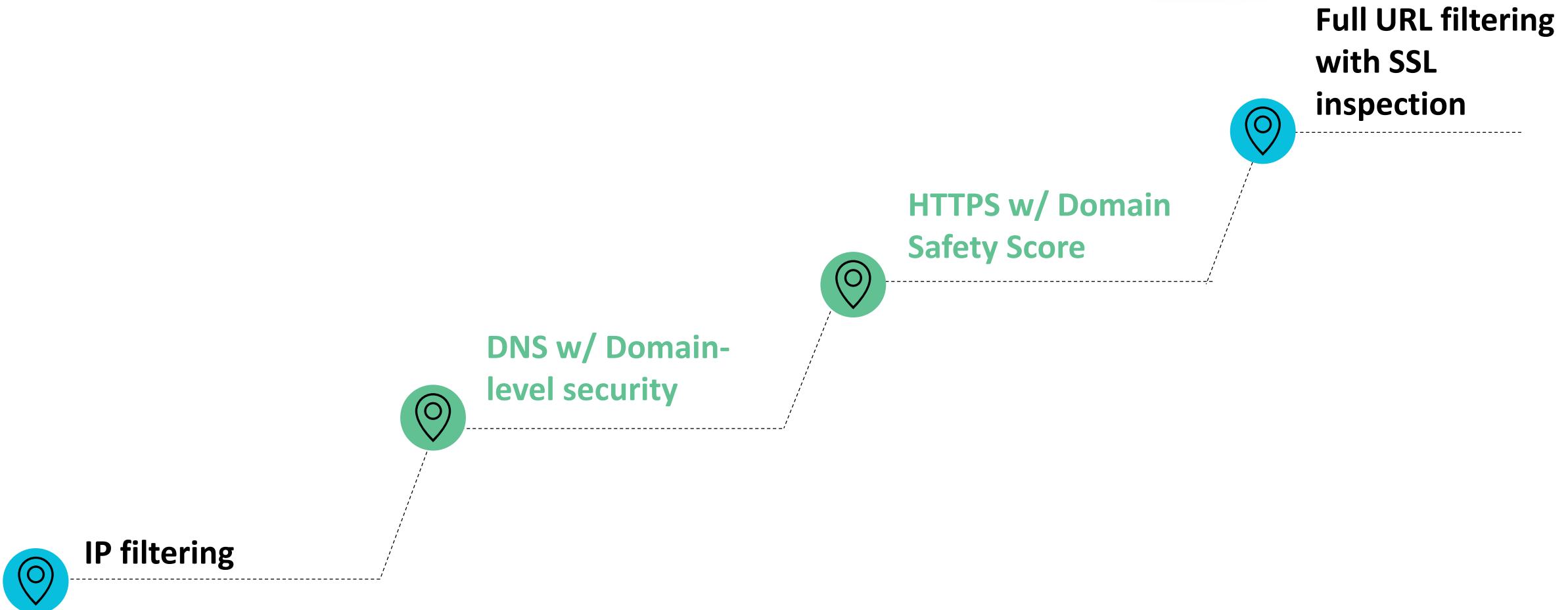
RSA®Conference2020

What the Future Holds

Current Solutions for Filtering on HTTPS Traffic



Filling the Gap: Classifying at the Domain Level



Recommendations to Security Professionals

			Domain level filtering
		Web filtering	Endpoint Security
Passwords	DNS / DoH	Patching	
Training		HTTPs	EDR / MDR
Phishing Simulations		Firewall	MFA
Outsourcing / leaning on the experts		VPN	Backup
USER		NETWORK	
			DEVICE

RSA®Conference2020

Thank you!
Questions?



**Continue the Discussion...
Visit booth S-635 for a conversation**