



Update on TLS SNI and IPv6 client adoption

March 20, 2018

Presenter: Erik Nygren, <nygren@akamai.com>



HTTPS Growth

Motivation

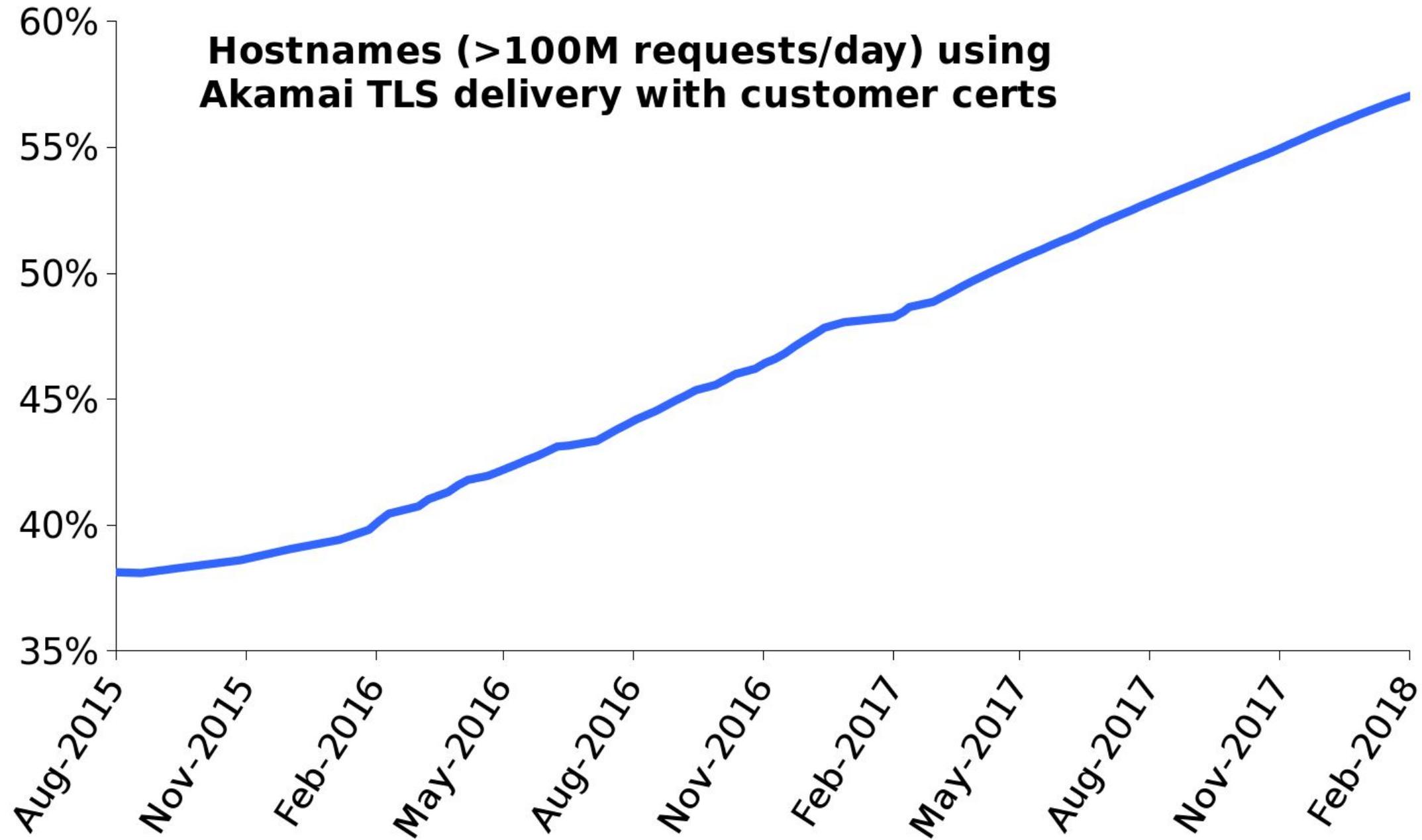
- HTTPS is growing rapidly but no IP multi-tenancy without TLS SNI
 - No indication of cert needed in TLS handshake without SNI
- IPv4 is exhausted at RIRs, but IPv6 still has a ways to go
- TLS SNI adoption was too low as a general solution until recently

HTTPS growth: from LetsEncrypt

- LetsEncrypt has 50M certs \Rightarrow equivalent of 3 /8's of IPv4 addresses
 - (TLS SNI and IPv6 are only sustainable ways forward)



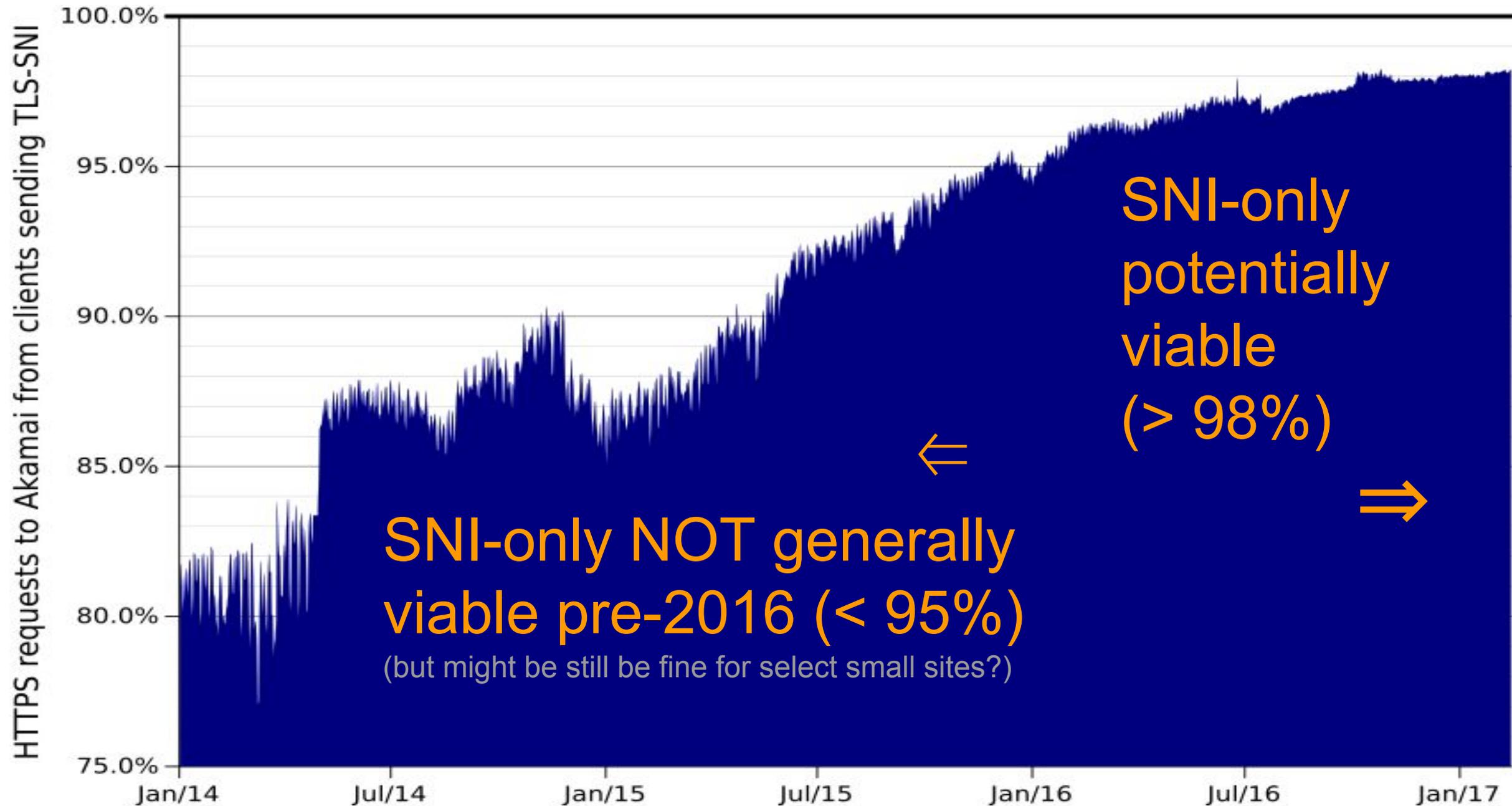
HTTPS transition of hostnames on Akamai over 3 years





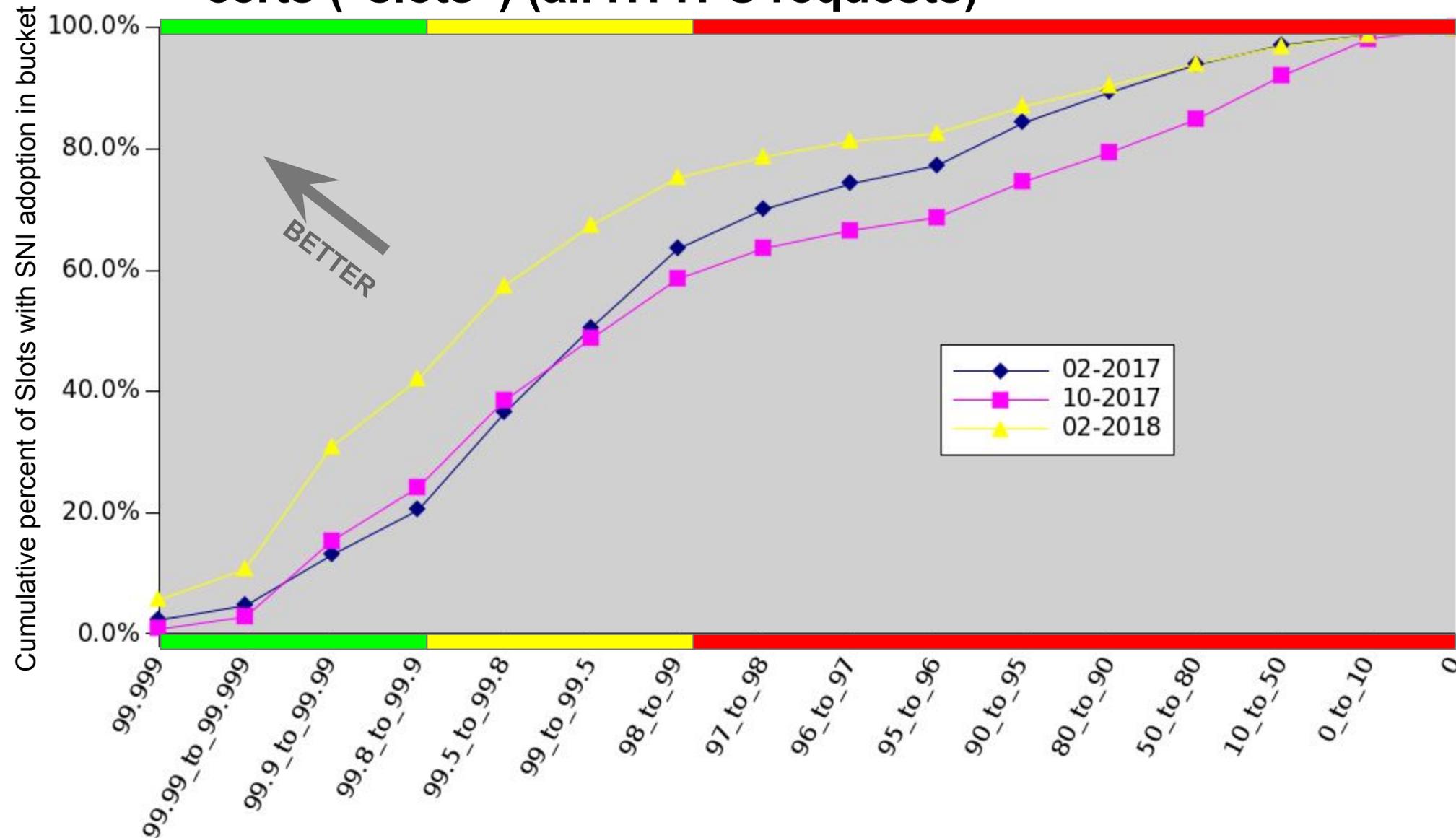
TLS SNI Trends

TLS SNI adoption: backstory on Non-SNI traffic



CDF of SNI usage on Akamai VIP-based customer certs (“slots”)

SNI adoption by number of VIP-based customer certs (“slots”) (all HTTPS requests)



31% of slots have SNI adoption over 99.9% (but 21% of slots below 97%)

Each line looks at ~8 Trillion HTTPS requests over the course of a week.

SNI adoption variation by country

- **No longer much global variation in Medians!**
 - (Past results had showed lower SNI usage in some countries)
- Median customer slot over 99.7% almost all geo-regions (99.76% globally)
- Median customer slot near/past 99.9% in many countries
- Lower median in China was fixed Fall 2017 (much was due to one search engine)
- For reference/context, median customer slot TLS 1.2+ usage is lower at 99.14%
 - Many TLS 1.0 clients do send TLS SNI, but some TLS 1.2 clients do not

What doesn't send TLS SNI?

- Custom clients and apps (eg, gaming consoles & anti-virus apps)
 - Tend to be customer-specific (ie, do not hold back general SNI usage)
- Spoofed User-Agents & MitM (eg, Anti-Virus, SWG) next top offenders*
- Windows XP now less than 6% of non-SNI traffic*
- Older Python & older Java/Apache-HttpClient around 4% of non-SNI*
- Almost all major search bots now have SNI support
 - Only one smaller Chinese search engine remains
- Very long tail of others...
 - Anecdotally, some are getting fixed (eg, ApacheBench)

** on slots with > 98% SNI*



IPv6 Trends

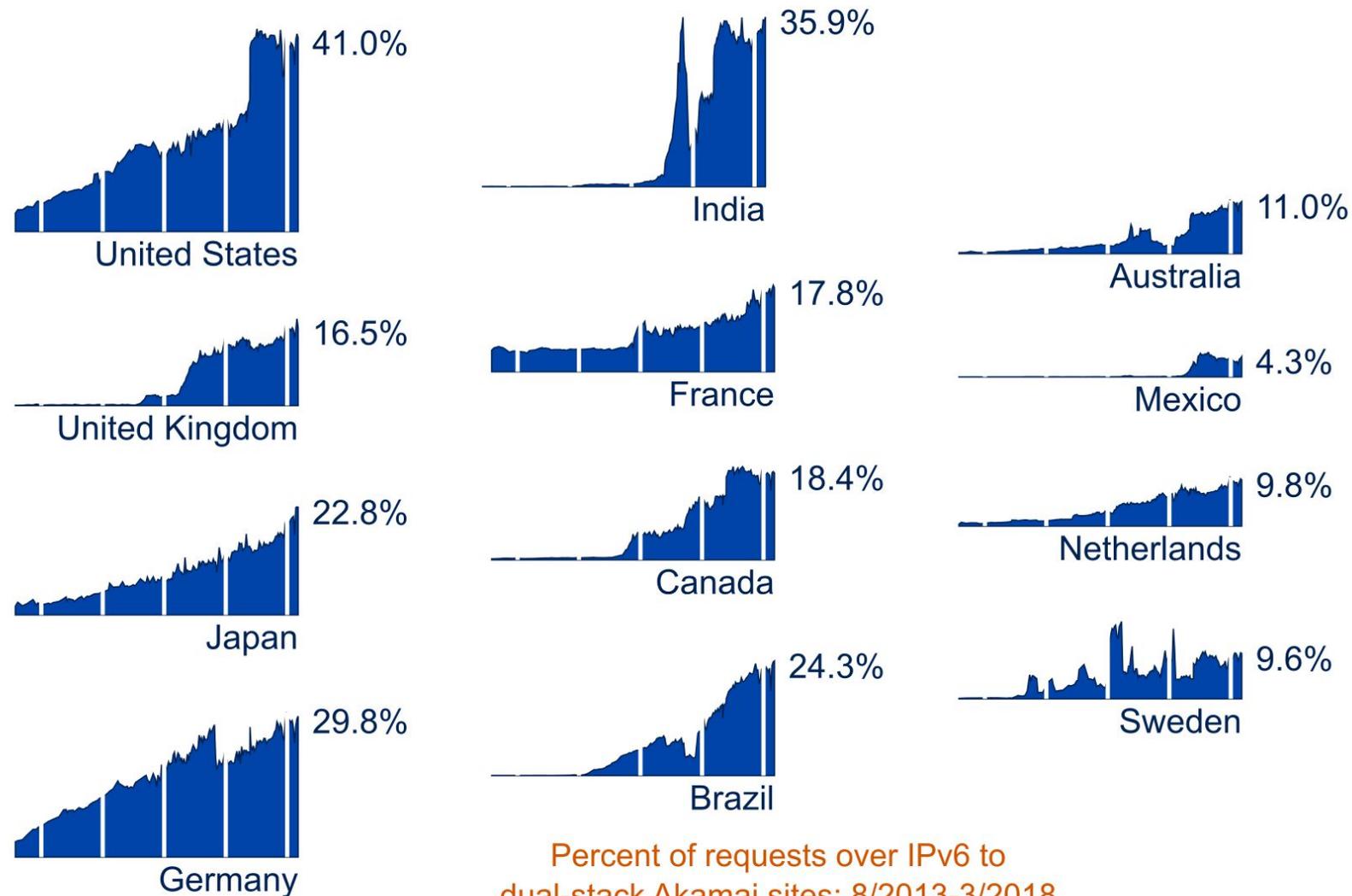
- Methodology: analyze 24-hour snapshots weekly (Wednesdays)
 - Data set contains a few hundred billion HTTP(S) requests against dual-stacked web sites
 - Looking at “IPv6 hits / Total hits”

Moving the needle? (of global average in 17% to 31% range)

- Approach: look at areas with top residual IPv4 traffic
- Two clusters:
 - IPv6 deployments already in-progress (tend to be on-top)
 - Little-to-no IPv6 deployed yet
- Heavily influenced by which ISPs/networks have deployed IPv6
- Exact percentages sensitive to content mix

Moving the needle: Countries with top residual IPv4

High IPv6 (and still significant opportunity)



Very limited IPv6 (< 3%)

(all below top-10 with IPv6)

- Russia
- China
- Italy
- Spain
- Indonesia
- Turkey
- South Korea

Moving the needle: Devices (vs. global average in 17% to 31% range)

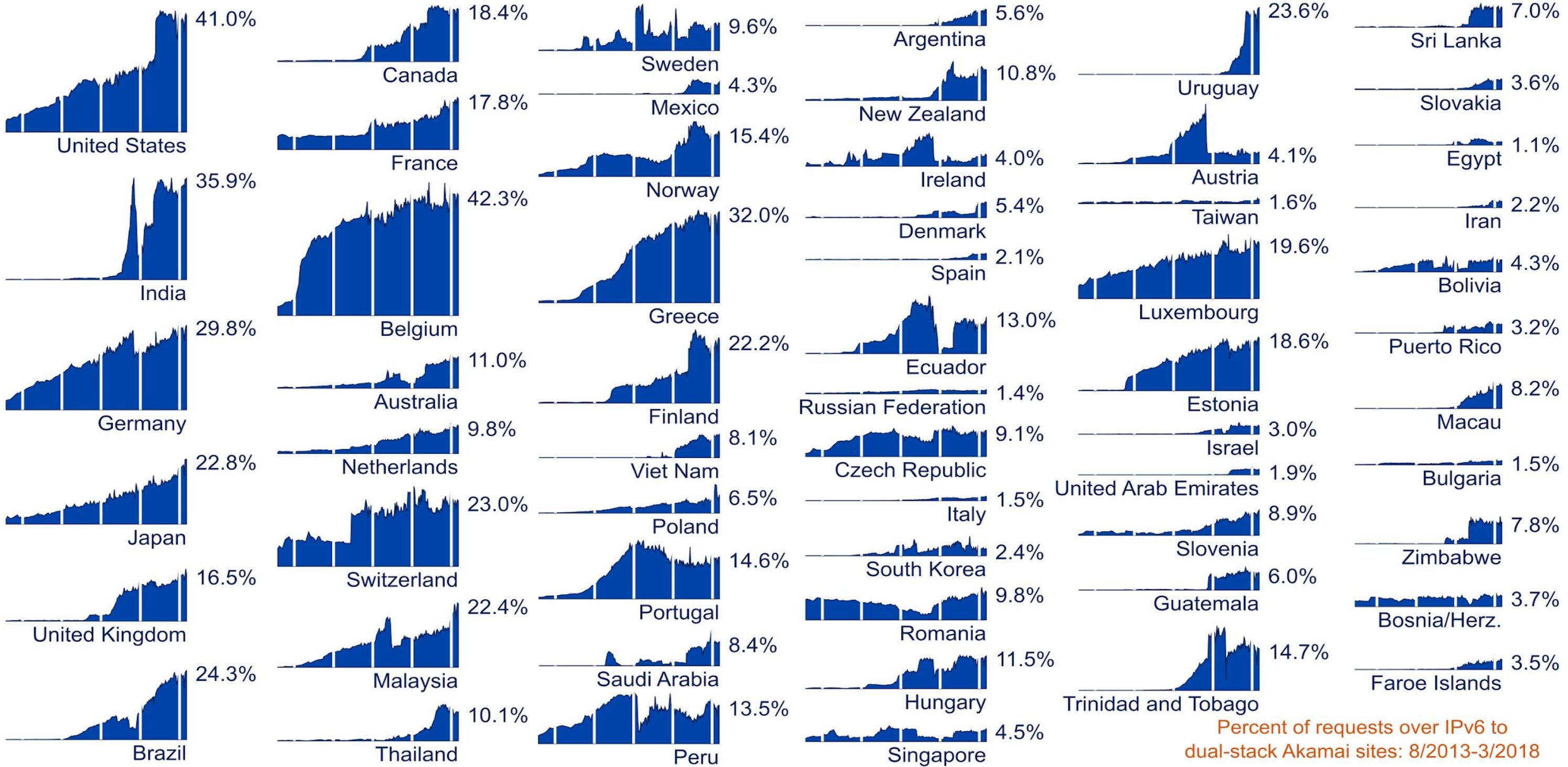
High IPv6 (but still opportunities) [with current approx. IPv6 pref.]	Very limited IPv6
<ul style="list-style-type: none">● Apple iOS 11 [28%]● Windows 10 [17%]● Windows 7/8.1 [9%]● Android 7 [29%]● Android 6 [25%]● Mac OS X 10.13 [24%]	<ul style="list-style-type: none">● Some streaming set-top boxes● Custom apps

Learning more

- **TLS SNI:** <https://bit.ly/2pbTWXF> <https://bit.ly/2FmBraG>
- **IPv6:** <https://akamai.com/ipv6>
- Questions?
 - Erik Nygren <nygren@akamai.com>

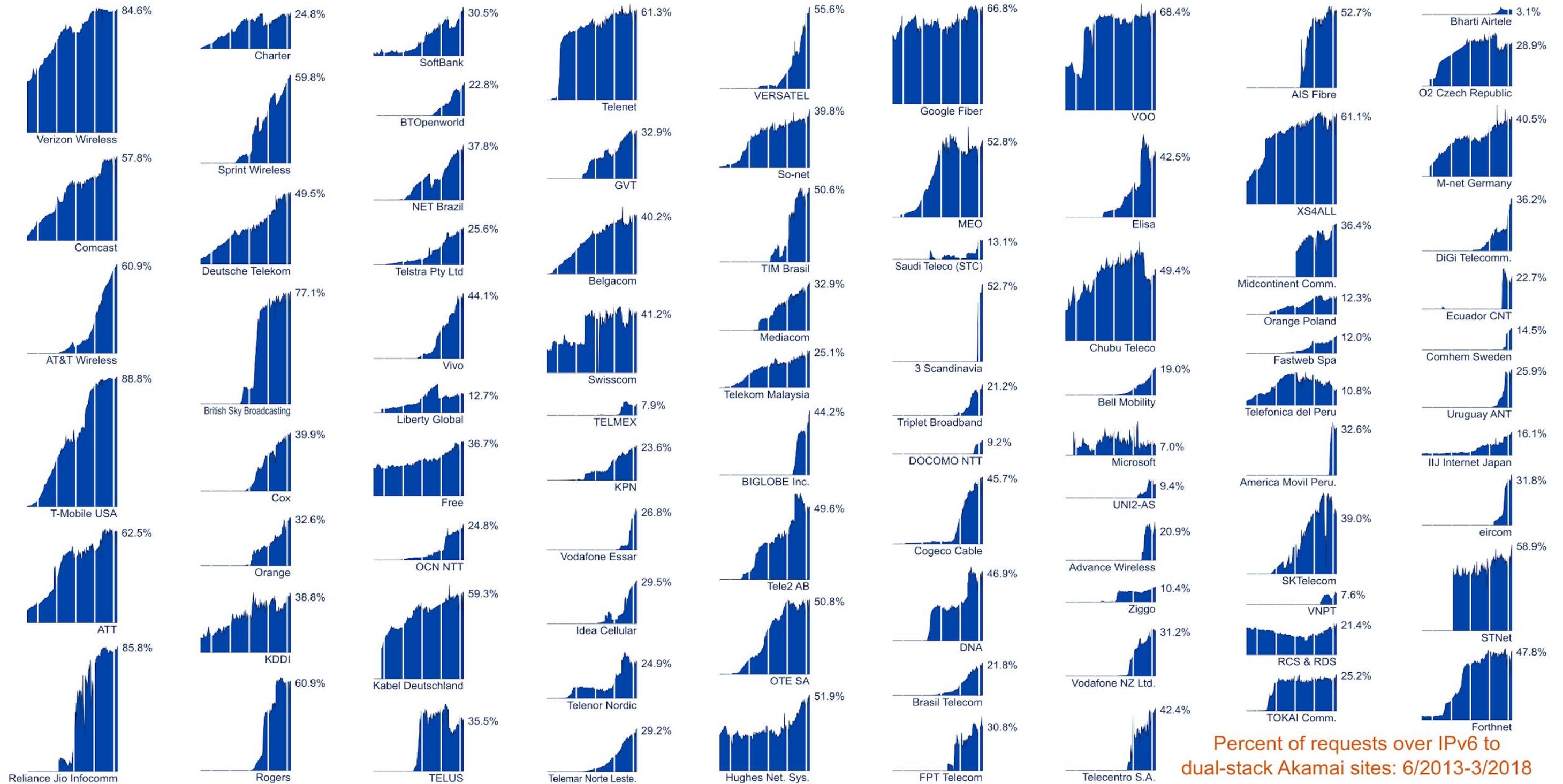
SUPPORT / BACKGROUND

Five years of IPv6 growth by country



Percent of requests over IPv6 to dual-stack Akamai sites: 8/2013-3/2018

Five years of IPv6 growth by network



Percent of requests over IPv6 to dual-stack Akamai sites: 6/2013-3/2018