

White-labeling in Telematics Project Update



Jaime Lightfoot

Cybersecurity Researcher
Lightfoot Labs



Anne Zachos

Cybersecurity Research Engineer
NMFTA

NMFTA's White-Labeling in Telematics project found:

**~50% of FMCSA-registered ELDs
support white-labeled hardware**
from the same few manufacturers

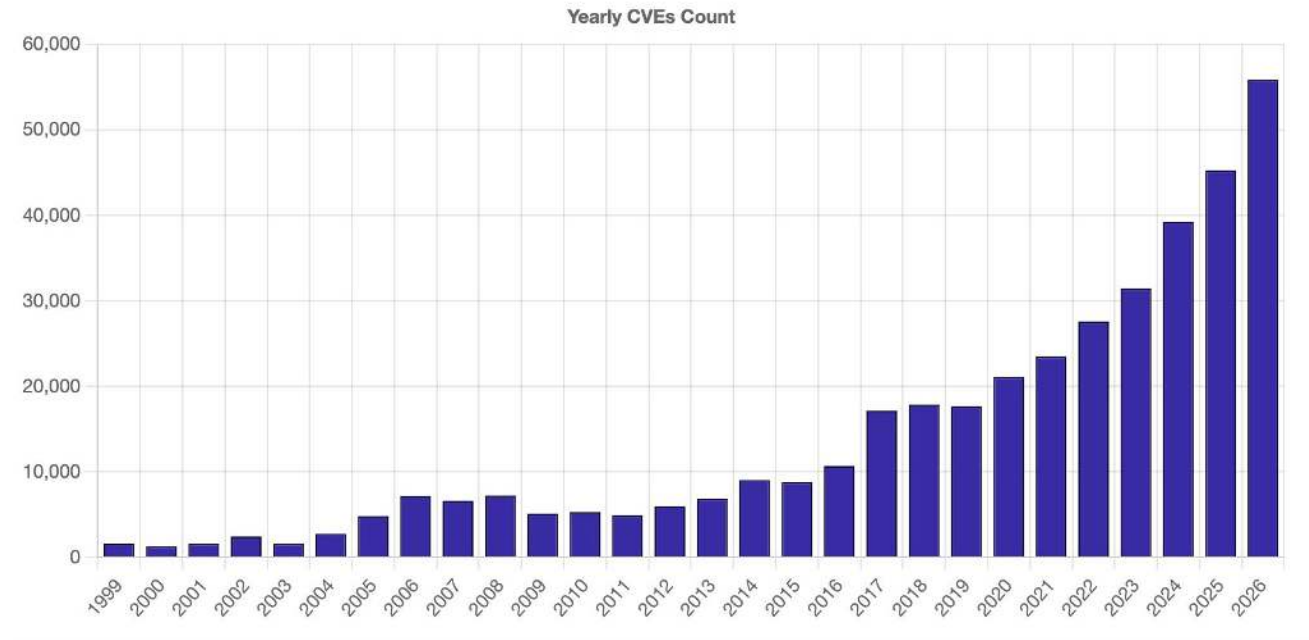
**~75% of the analyzed ELDs use
white-labeled software**
from a pool of ~20 white-labeling companies

Motivations

- ELDs required for vast majority of trucks on the road
- Lack of cybersecurity scrutiny and published research
- Want to identify shared risk across all parts of ELD ecosystem

Why This Matters Now

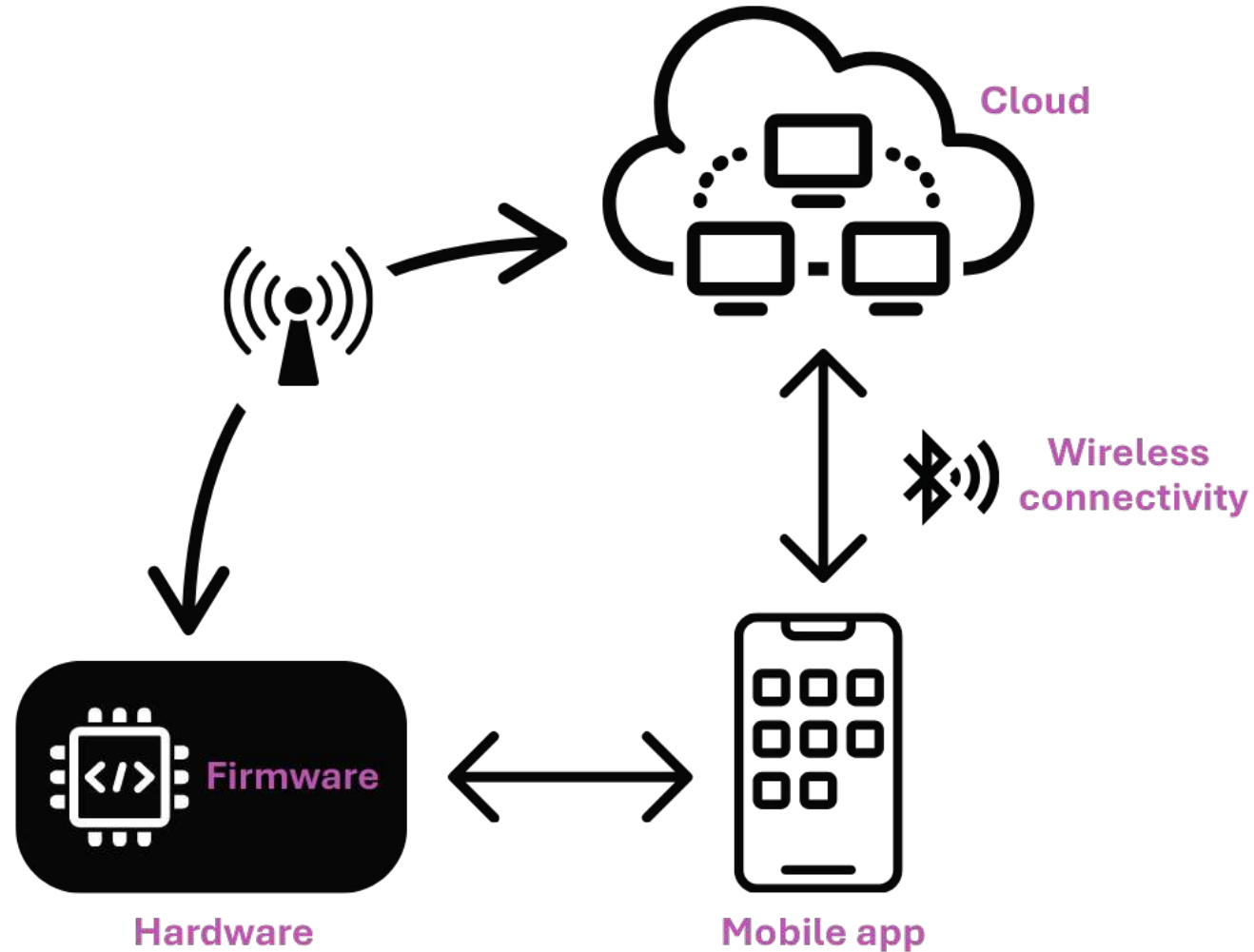
- Large increase in CVEs
- Rising threats in trucking
 - Ransomware, cargo thefts, etc
- Asset side may become target
- ELD risks:
 - Vehicle attacks
 - Privacy concerns
 - Compliance issues



Graph from OpenCVE

Shared Risk

- Looking at shared risk across entire ELD ecosystem



Methodology

- Research project over the course of 1 year
 - Including entire FMCSA list, with 67 revocations and 6 additions
- Hardware from donations and/or Ebay
- Mobile apps (APKs) downloaded from app store and mirror sites
- ELD provider manuals and images from FMCSA site
- Not a pentest

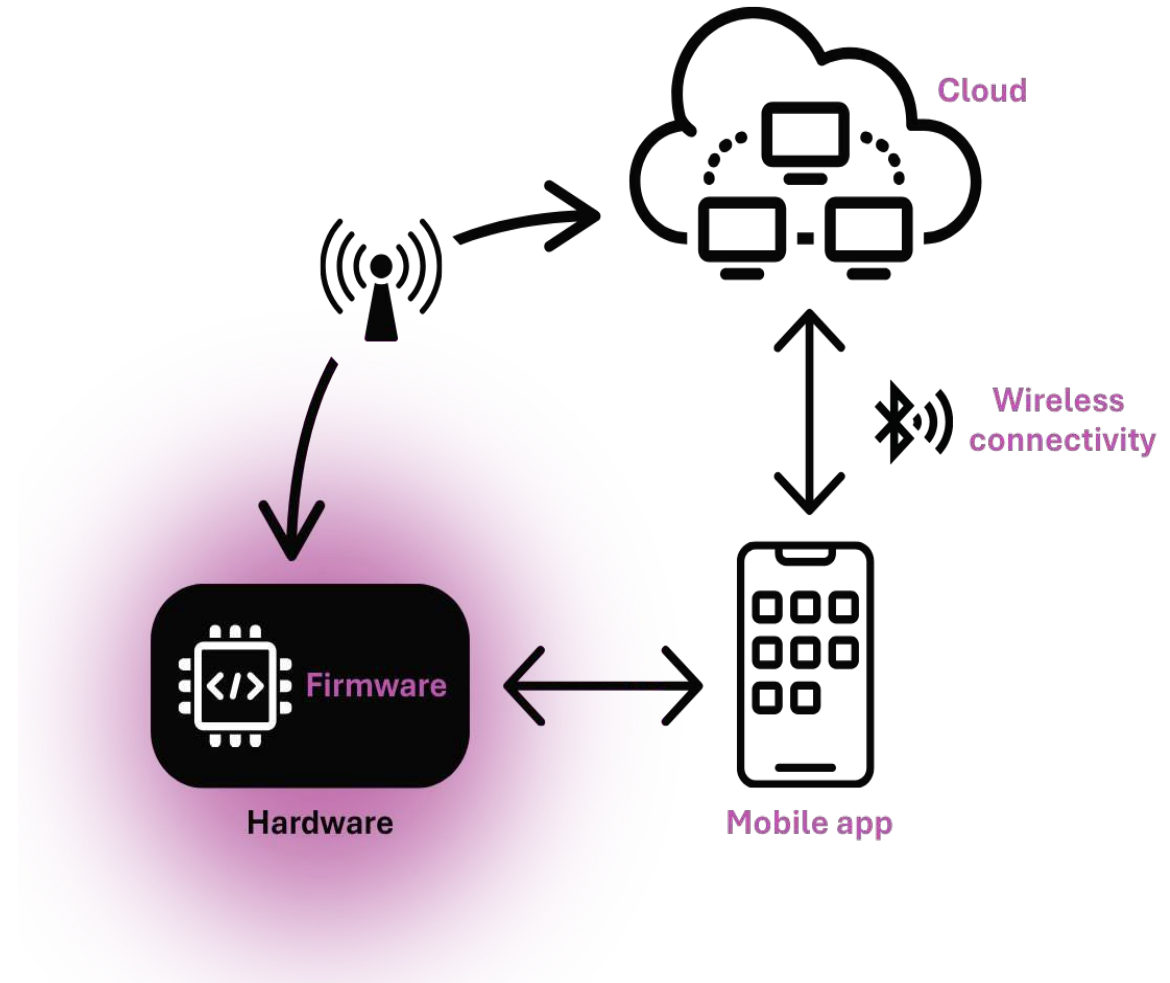
Hardware

Shared risk questions:

- Are HW vendors selecting same chips?
- How unique are hardware designs?

Why this matters:

- Vulnerabilities in hardware are very hard to fix
- Wireless chips often ship with stock firmware (high-value targets)



Hardware Reverse Engineering

- Had hardware from a dozen brands
- Disassembled and identified all components



Hardware Findings

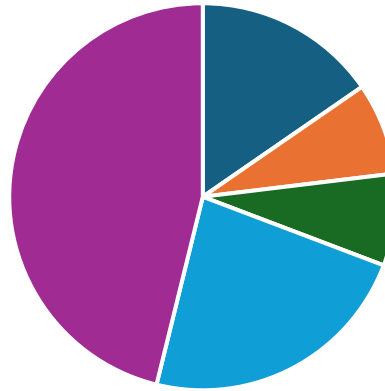
- Healthy diversity of hardware choices
 - Few-to-none shared components within manufacturer groupings/families

MCU Manufacturers



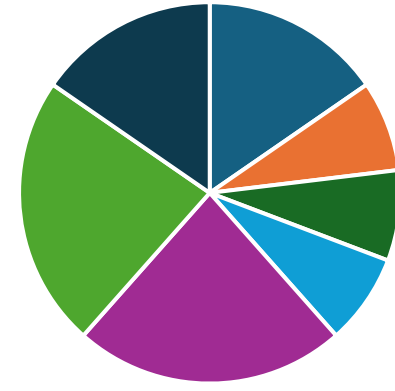
■ Texas Instruments ■ STMicro ■ NXP ■ Espressif ■ Microchip

LTE Modem Manufacturers



■ Sierra Wireless ■ U-Blox ■ WNC ■ Quectel ■ N/A

Bluetooth/WiFi Manufacturers

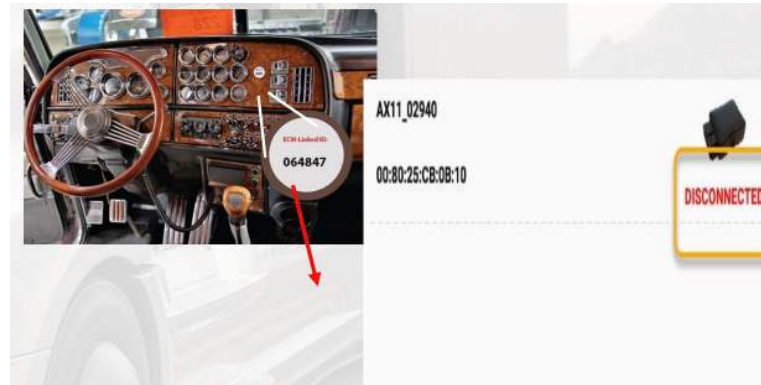


■ Texas Instruments ■ Nordic ■ Quectel
■ Panasonic ■ Espressif ■ Other Manufacturers
■ Unknown

- No obvious white-labeling or design copying among major players

Hardware White-labeling

- Major players aren't white-labeling
 - Still leaves 95% of the FMCSA by count
- Can we identify all hardware manufacturers from FMCSA list?



Screenshots from FMCSA List



Hardware White-labeling: FMCSA List

- Same few white-labeled HW makers dominate FMCSA list
 - 44% of ELDs on FMCSA list support Pacific Track devices
 - ~60% of ELDs support 5 most common white-labeled HW

Hardware Supplier	ELDs	% of FMCSA List
Pacific Track	451	44.2%
IOSiX	84	8.2%
Geometris	70	6.9%
CalAmp	38	3.7%
BlueLink	23	2.3%
Others	47	4.6%

FMCSA List Share by Hardware Type
(Source: FMCSA PDFs and photos)



Hardware White-labeling: SDKs

- Manuals and photos provided to FMCSA not always thorough
- Can we find a better way to enumerate hardware support?
- Yes: by finding ELD device connection code in mobile app
 - Known as SDK or Software Development Kit
 - Code library provided by hardware vendor to speed up development time

Hardware White-labeling: SDKs

- Share of FMCSA list by software dev kit code found in ELD apps:

HW SDK Name	ELDs	% of FMCSA List	App Downloads
Pacific Track SDK	518	50.7%	439k
IOSiX SDK	440	43.1%	480k
Suntech	275	26.9%	210k
CalAmp	102	10.0%	153k
Geometris	119	11.7%	192k
Raven	66	6.5%	68k
ELDBox	66	6.5%	98k
Xirgo	60	5.9%	237k

FMCSA List Share by Hardware Type
(Source: ELD App SDKs)

Hardware Takeaways

- Didn't find white-labeling in big players
- Half of list uses white-labeled hardware from same 3-5 suppliers

Hardware Supplier	ELDs	% of FMCSA List
Pacific Track	451	44.2%
IOSiX	84	8.2%
Geometris	70	6.9%
CalAmp	38	3.7%
BlueLink	23	2.3%
Others	47	4.6%

FMCSA List Share by Hardware Type
(Source: FMCSA PDFs and photos)

HW SDK Name	ELDs	FMCSA List %	App Downloads
PT SDK	518	50.7%	439k
IOSiX SDK	440	43.1%	480k
Suntech	275	26.9%	210k
CalAmp	102	10.0%	153k
Geometris	119	11.7%	192k
Raven	66	6.5%	68k
ELDBox	66	6.5%	98k
Xirgo	60	5.9%	237k

FMCSA List Share by Hardware Type
(Source: ELD App SDKs)

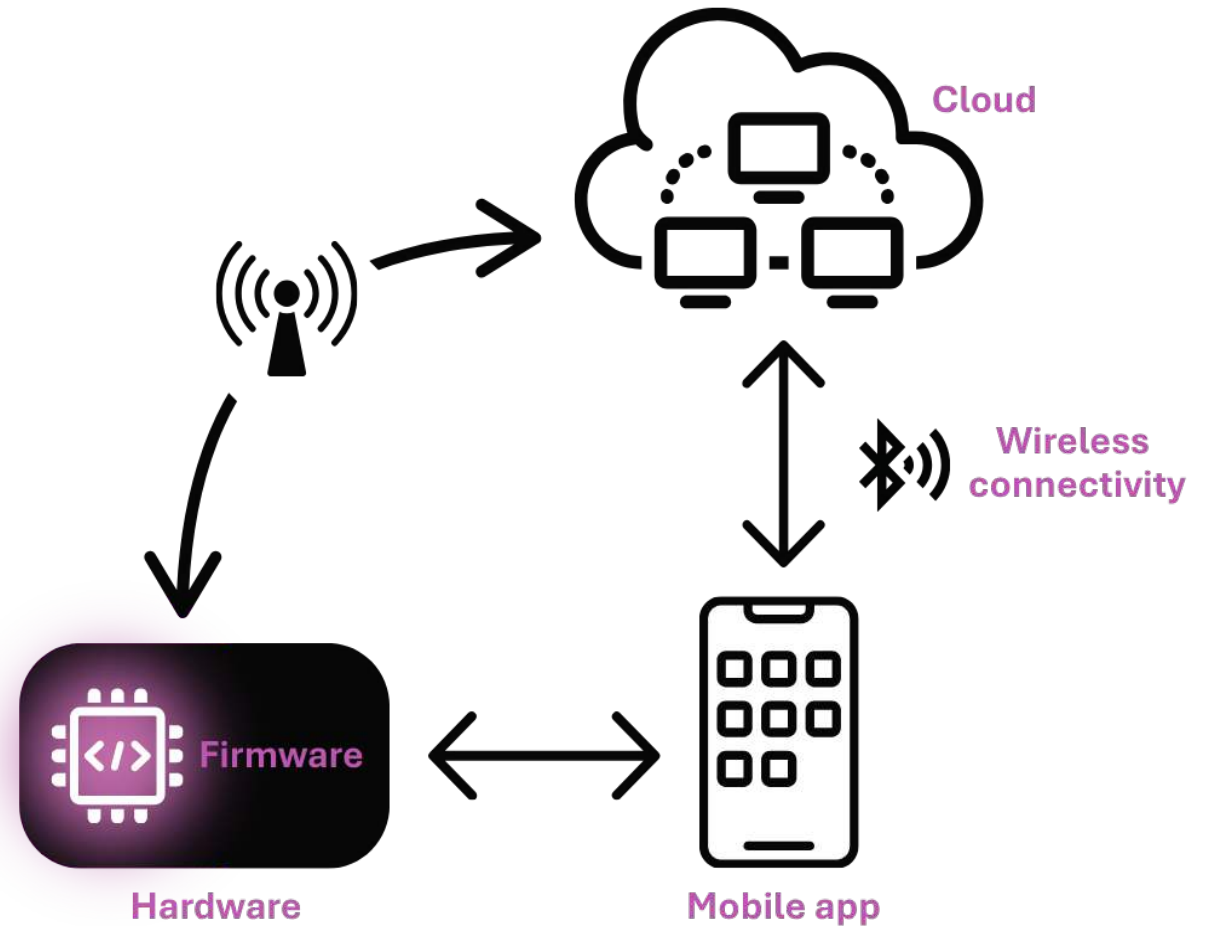
Firmware

Shared risk questions:

- Are similar libraries in use across many ELDs?
- Shared architecture across providers?

Why this matters:

- Shared libraries focus of AI analysis
- Vulnerabilities in connectivity-related libraries = way to influence truck behavior



Firmware Extraction

- Engineers need a way to program devices
- Security best practice to lock those methods in production
 - Not the case for majority of ELDs we reverse engineered
- Able to extract 12 firmware binaries
- Used VicOne xZETA to generate SBOMs for each device

Firmware SBOMs: Complex Devices

- Standard libraries commonly used
 - Standard C libraries, hardware interfacing, networking, cryptography, system utilities and storage
- Multiple versions of some packages

Library name
attr
bash
bluesz
busybox
can-utils
curl
dbus
e2fsprogs
glibc
hostapd
iproute2

Library name
iptables
iw
lvm2
mtd-utils
openssl
pcre
sqlite
tcpdump
util-linux
wireless-tools

Firmware SBOMs: "Bare Metal" Devices

- Some shared libraries
 - FreeRTOS commonly used
 - Connectivity-related libraries <1/3 of samples
- Shared libraries mostly reflect common use of ESP32 hardware-related libraries

Library Name	Firmware Sample Matches
Free RTOS	8
lwIP	6
ESP-IDF	5
Espressif WiFi	5
RivieraWaves BT/BLE	5
Bluedroid	3
MBEDTLS	3
NimBLE	2
Others	2 or fewer

Firmware Takeaways

- Common open-source development libraries
- Some diversity within "bare metal" category
- Fallout of firmware shared risk:
 - AI means these libraries are easy to target
 - ELD updates will be important
 - Possible impact on truck safety

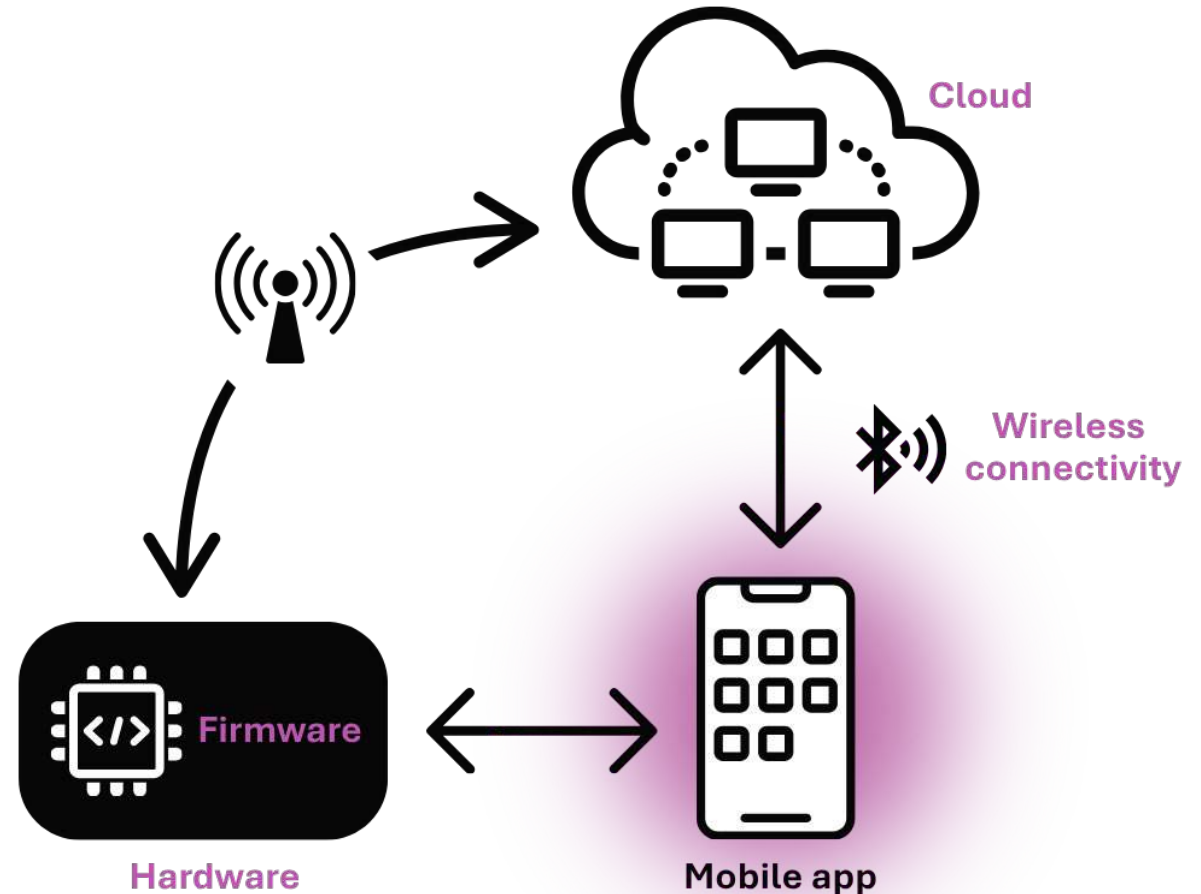
Mobile Apps

Shared risk questions:

- Are mobile apps white-labeled?
- What can we learn about cloud/other connections?

Why this matters:

- Mobile apps are gate through which lots of data flows:
 - Location, HOS records, downloads
- Lets us understand hardware and cloud connections

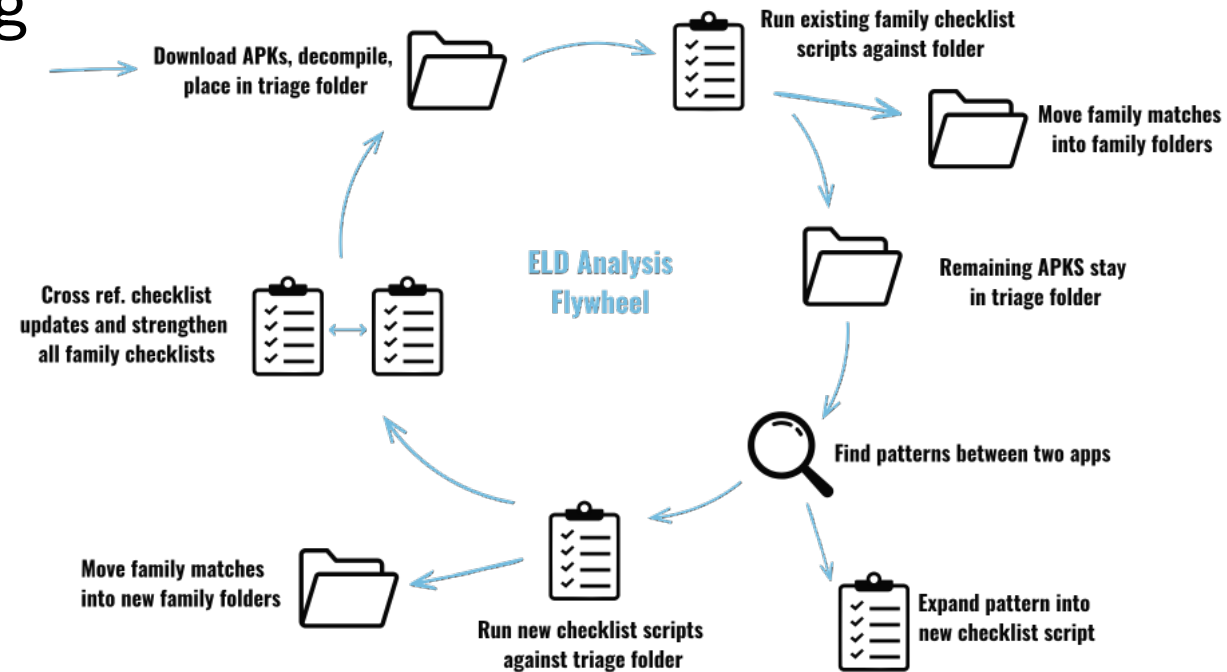


The Journey to Downloading Every ELD App

- Started as a hunt to find more firmware packages
- ELD mobile apps often facilitate firmware updates
 - Some fetch it on demand from the cloud
 - Some bundle it into the mobile app without encryption
- Started downloading mobile apps to find firmware for white-labeled hardware
 - Started noticing patterns

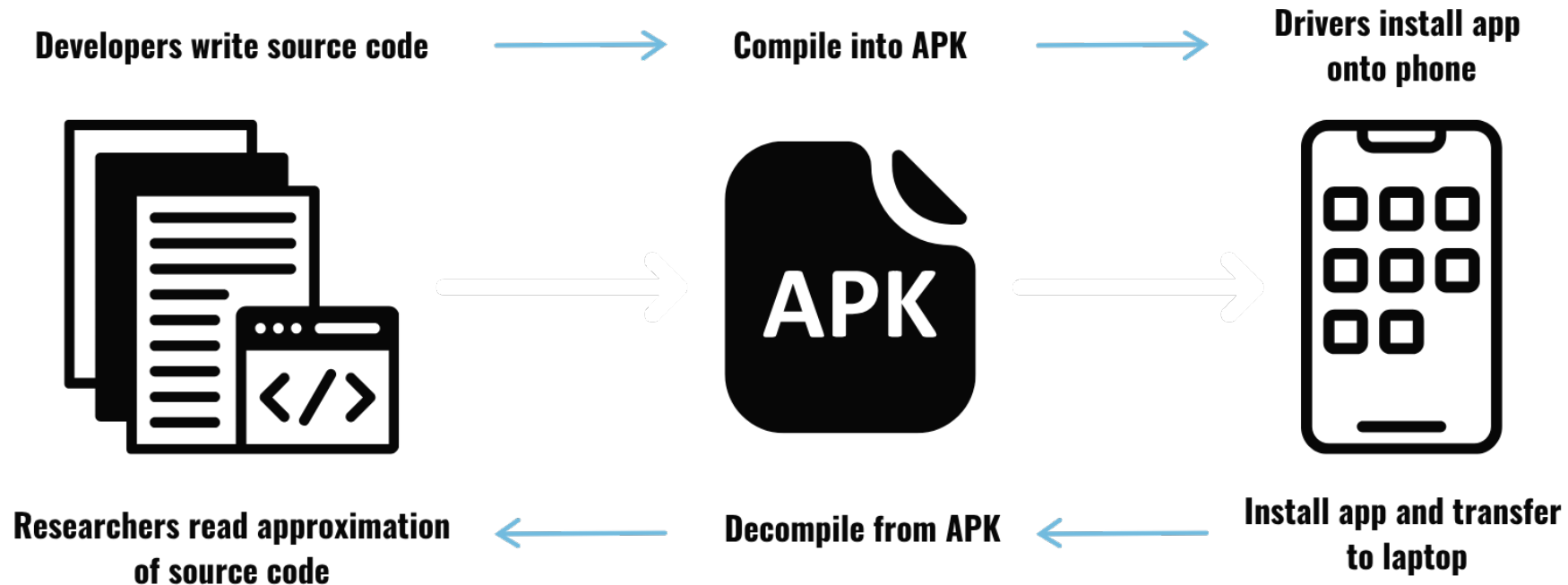
Mobile App Analysis

- Started with 10-15 apps, expanded to hundreds
- Started finding proof of white-labeling
- Created a flywheel:
 - Download mobile apps
 - Decompile
 - Compare against other apps
 - Formalize into checklist scripts
 - Automate process



Mobile App Analysis

- Able to compare ELD app code after de-compilation:



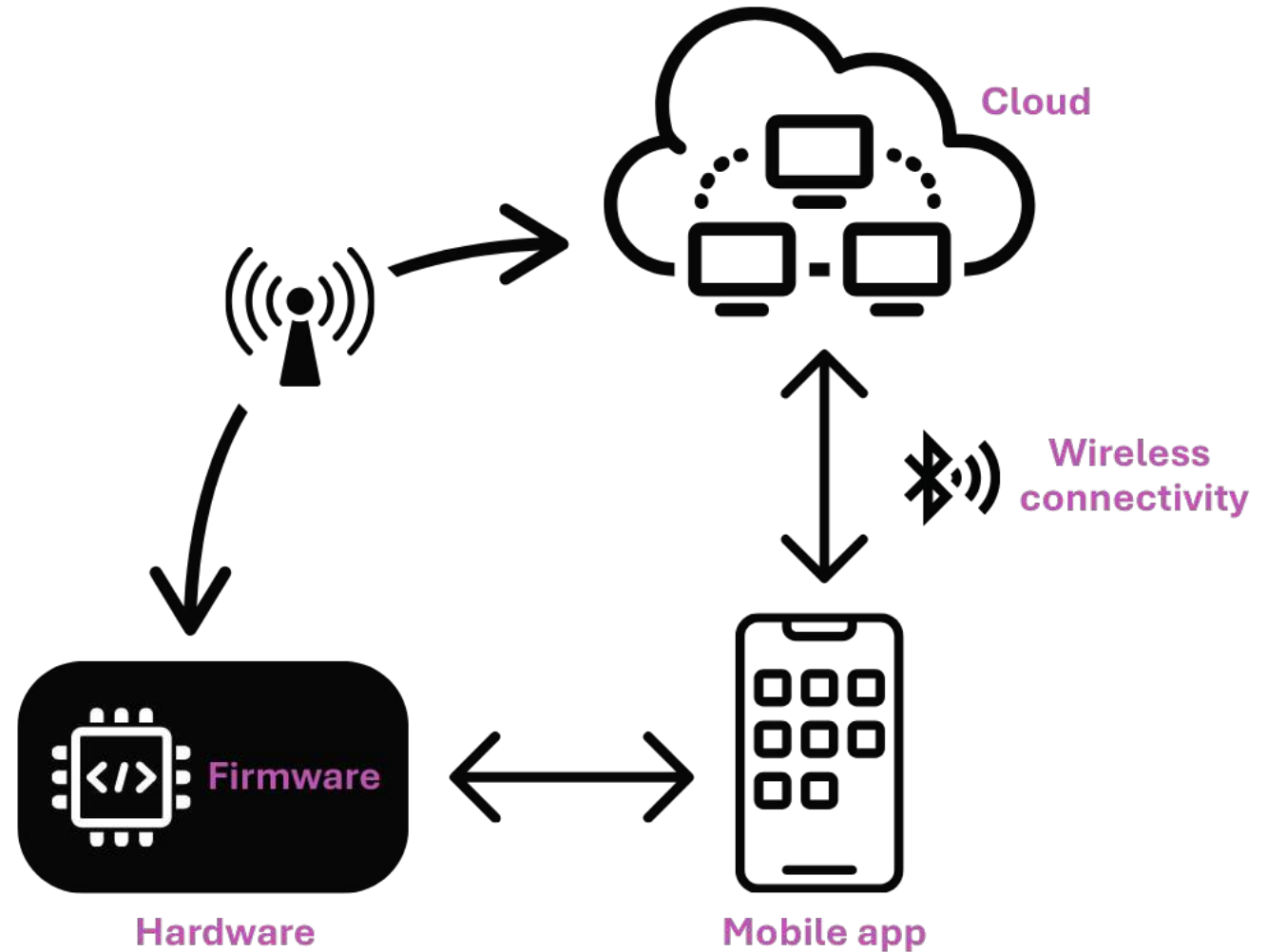
Mobile App Analysis

- Sped up flywheel further with AI
- Good for finding patterns in large amounts of easily-parsed data
 - XML files
 - Certificates
 - Commonly used strings
 - URL values for API calls
 - Software library choices
- Good for scripting, tedious comparisons, hashing, regexes

What We Can Learn from Mobile Apps

- White-labeler name/family
- Hardware connections
- Cloud connections
- 3rd party connections
- Development details

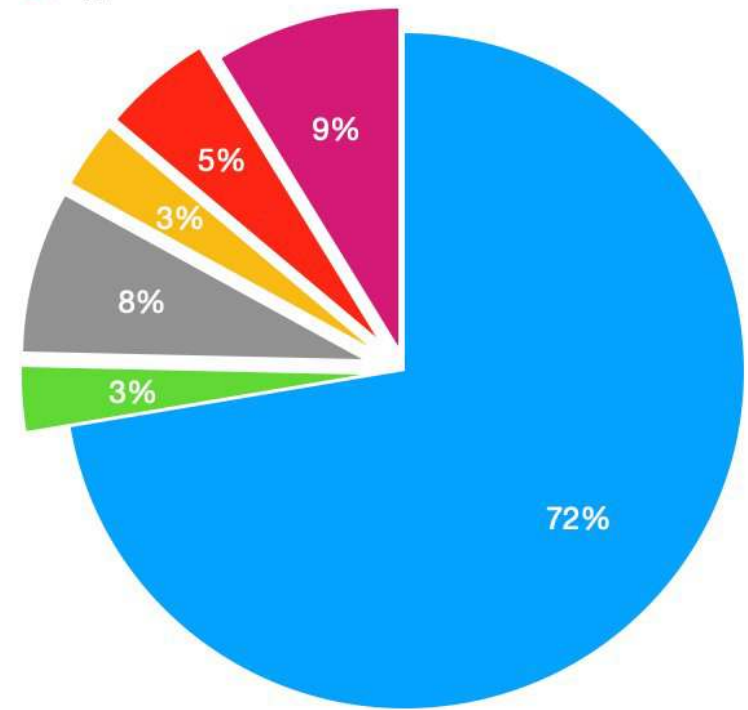
... all local to our computers



What We Covered

- 739 ELDs out of 1020 on FMCSA list
- Remainder missing because:
 - iOS only
 - Integrated tablet only
 - Enterprise portal gated
 - Defunct companies
 - Delisted from app store
 - Etc
- All stats shown are scoped to 72% region

- APK known + analyzed
- APK known but not downloadable
- iOS/Tablet/Enterprise only
- App unknown + LLC defunct
- App unknown + no LLC complaints + website/hosting defunct
- App unknown - other reasons

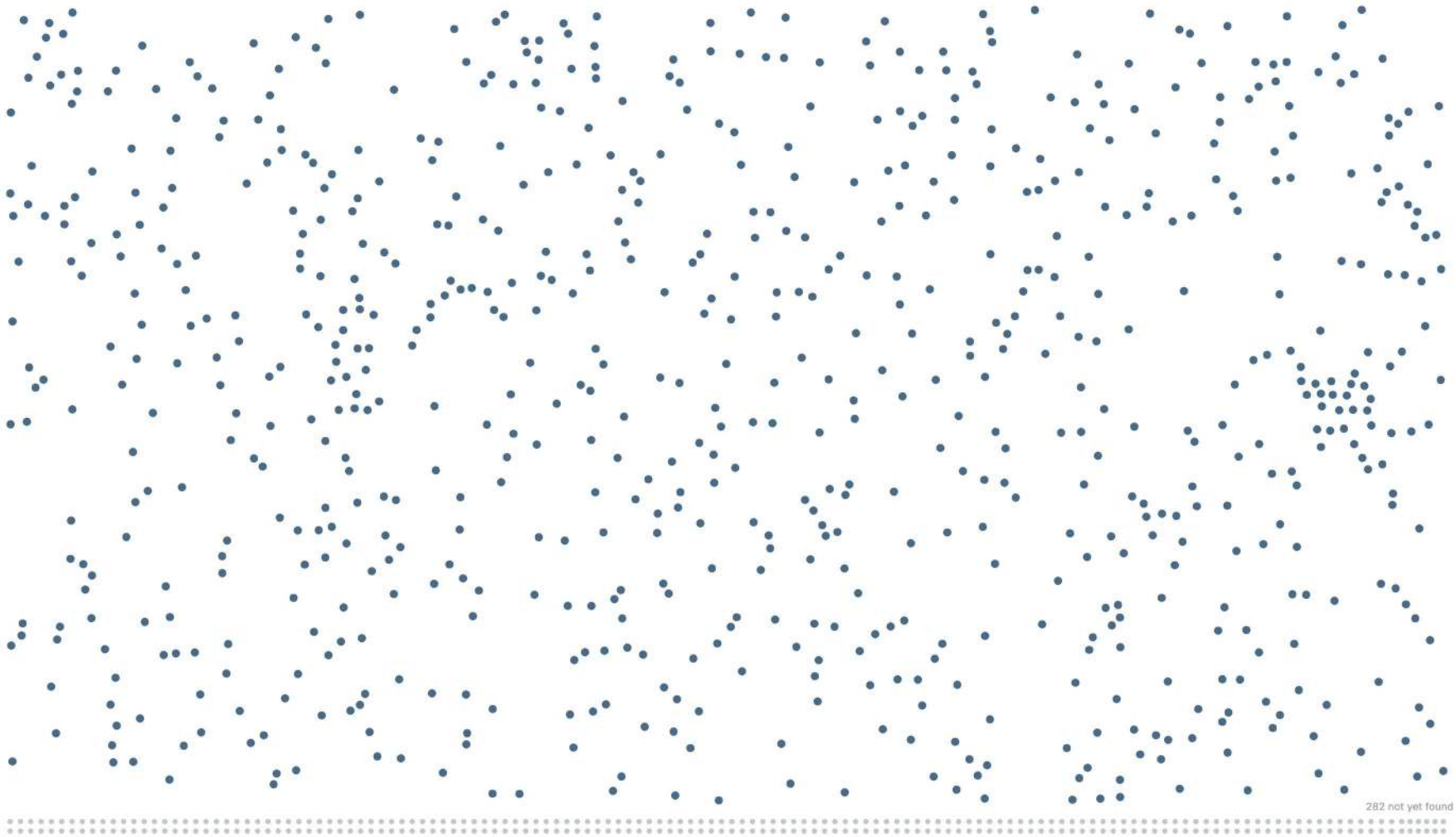


What We Found

- 75% of analyzed list are in white-labeled families
- 20+ families found, ranging from 4 to 170+ members
- White-labeling: same product resold by multiple different companies
- Family = functionally identical mobile app besides branding
 - Same mobile app logic, originating from same codebase
 - Same hardware support
 - Typically same/shared cloud resources: APIs, databases, storage
- Most/all of ELD ecosystem white-labeled, not just mobile app

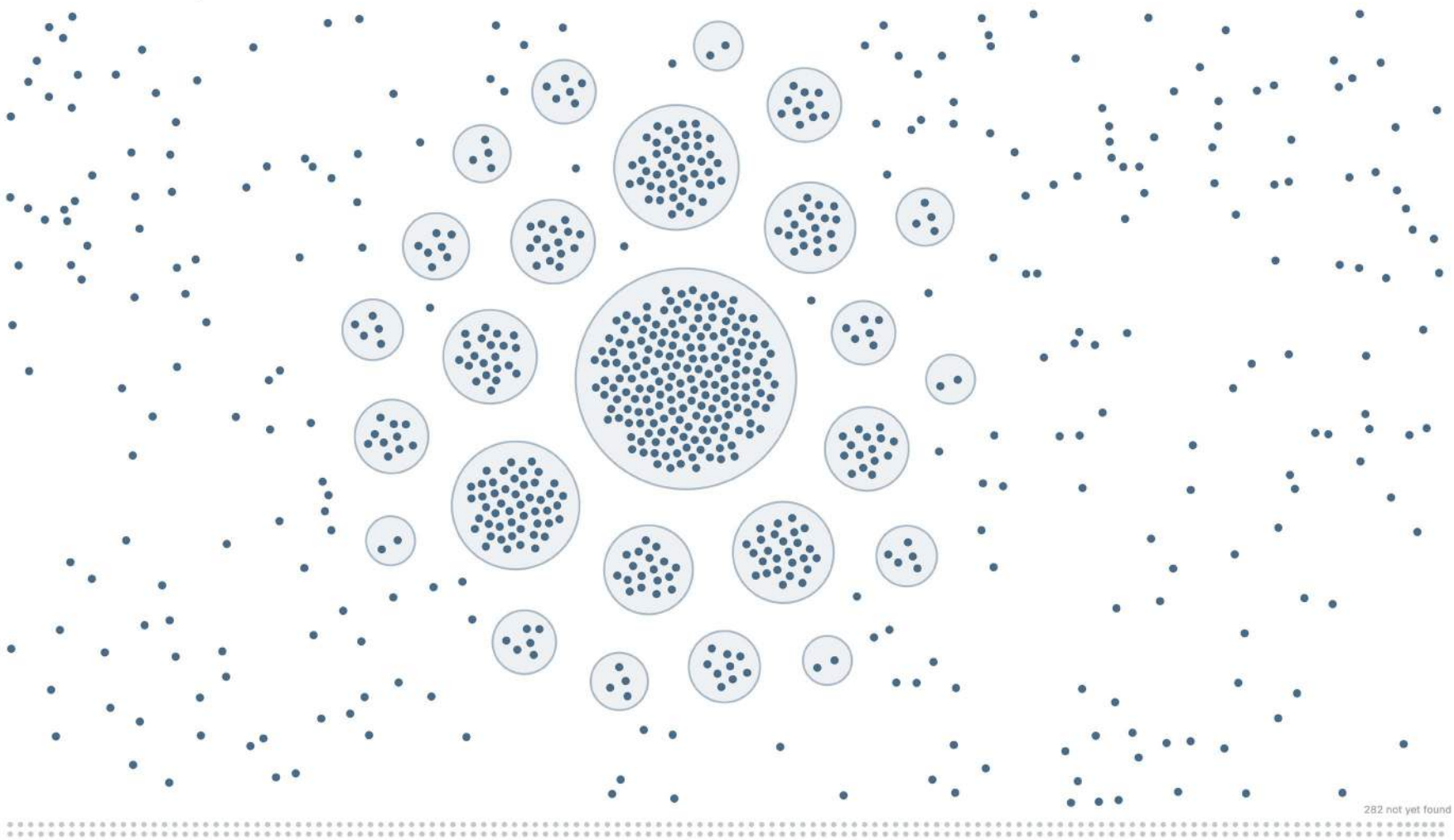
What We Found

ELD Market Landscape



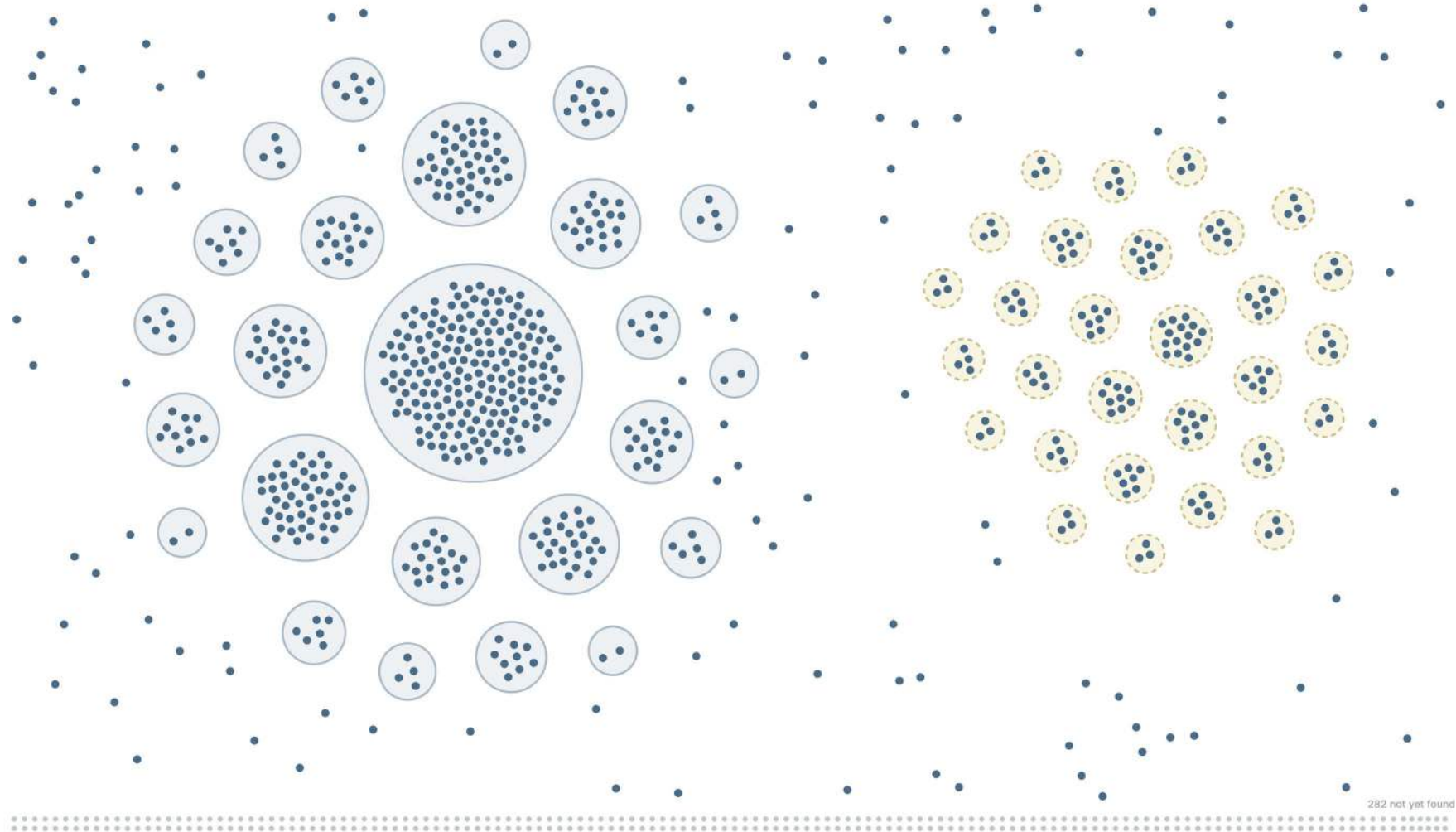
White-Labeled Families

ELD Market Landscape



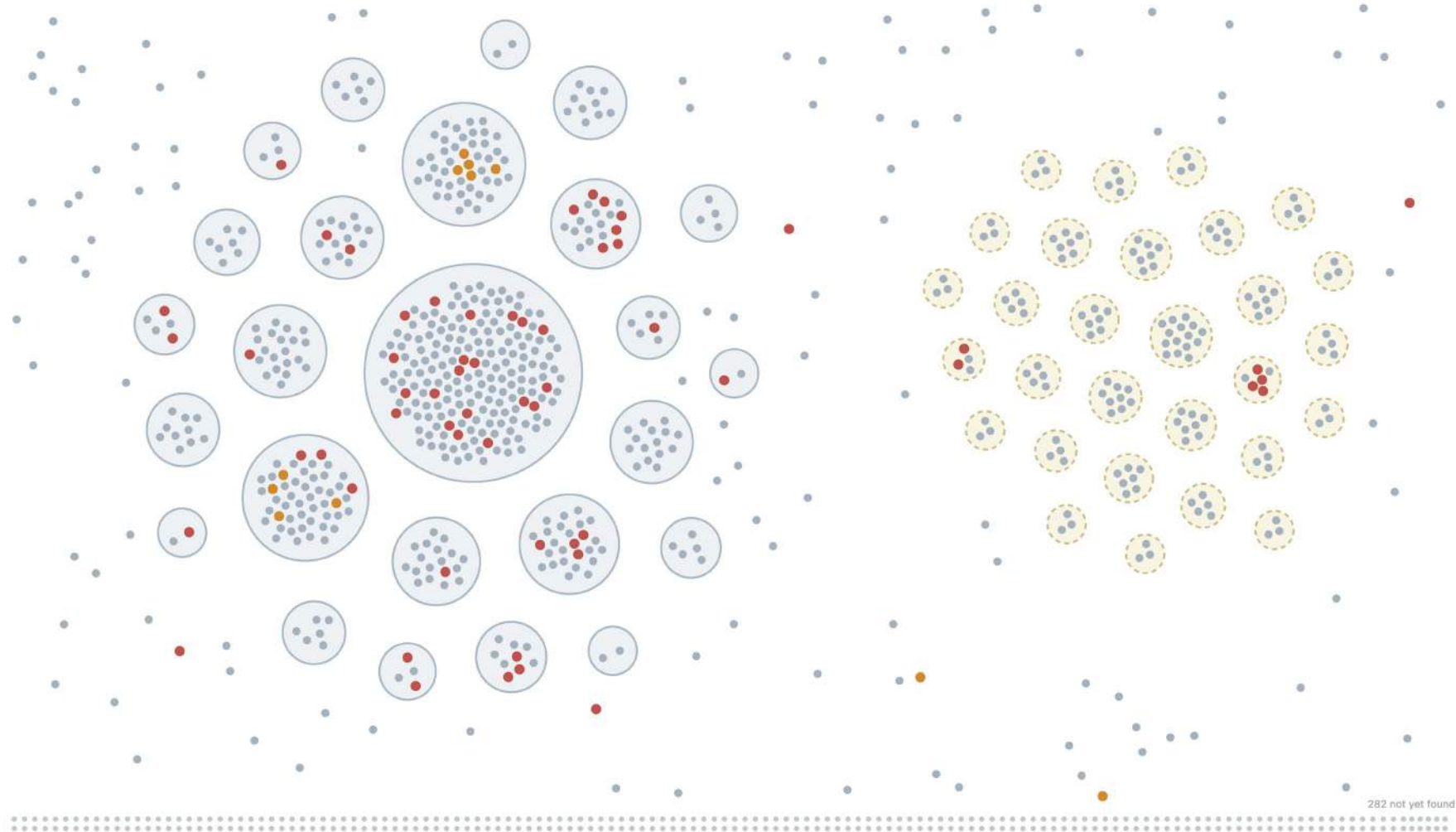
Families and Brands

ELD Market Landscape



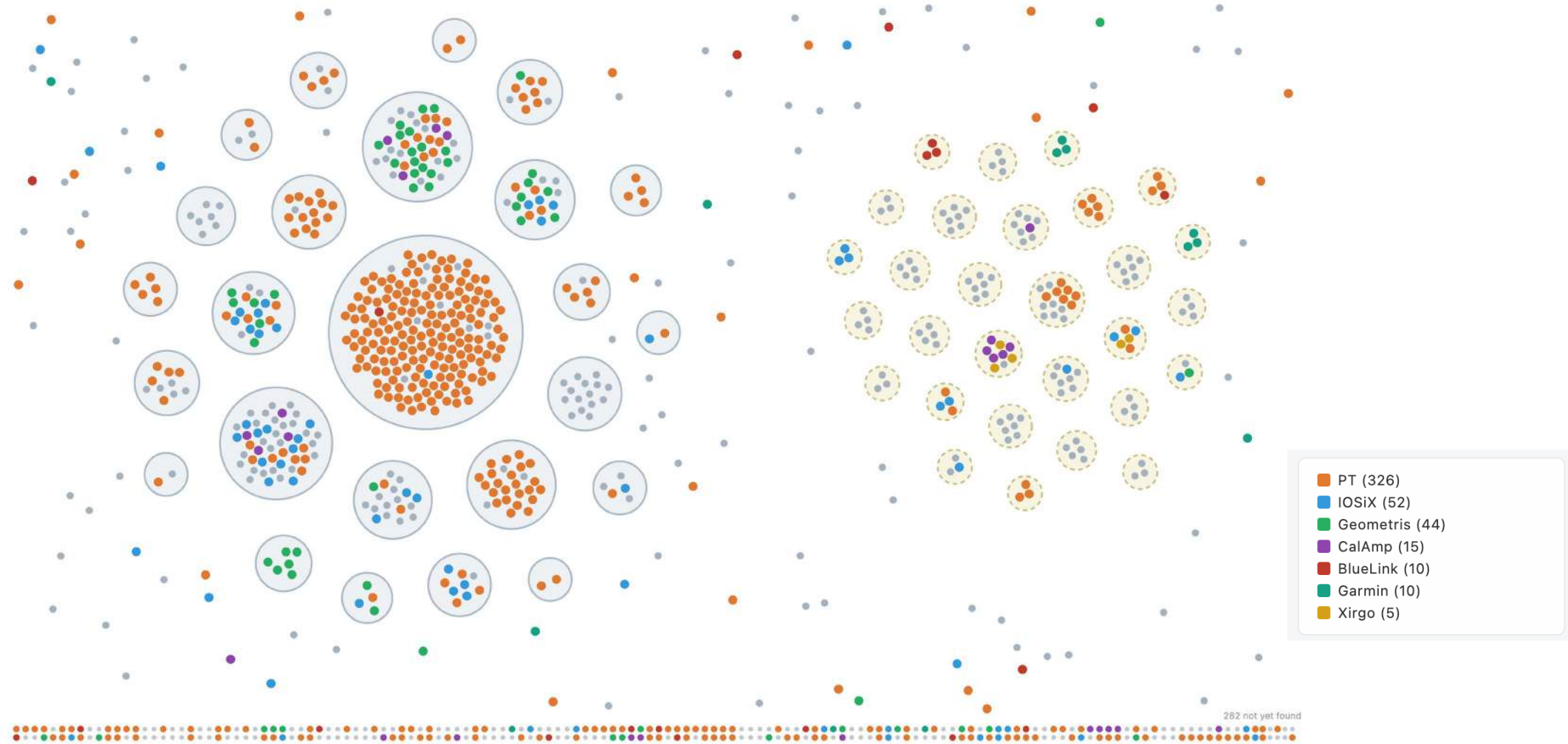
Revocations

Revoked ELD Registrations



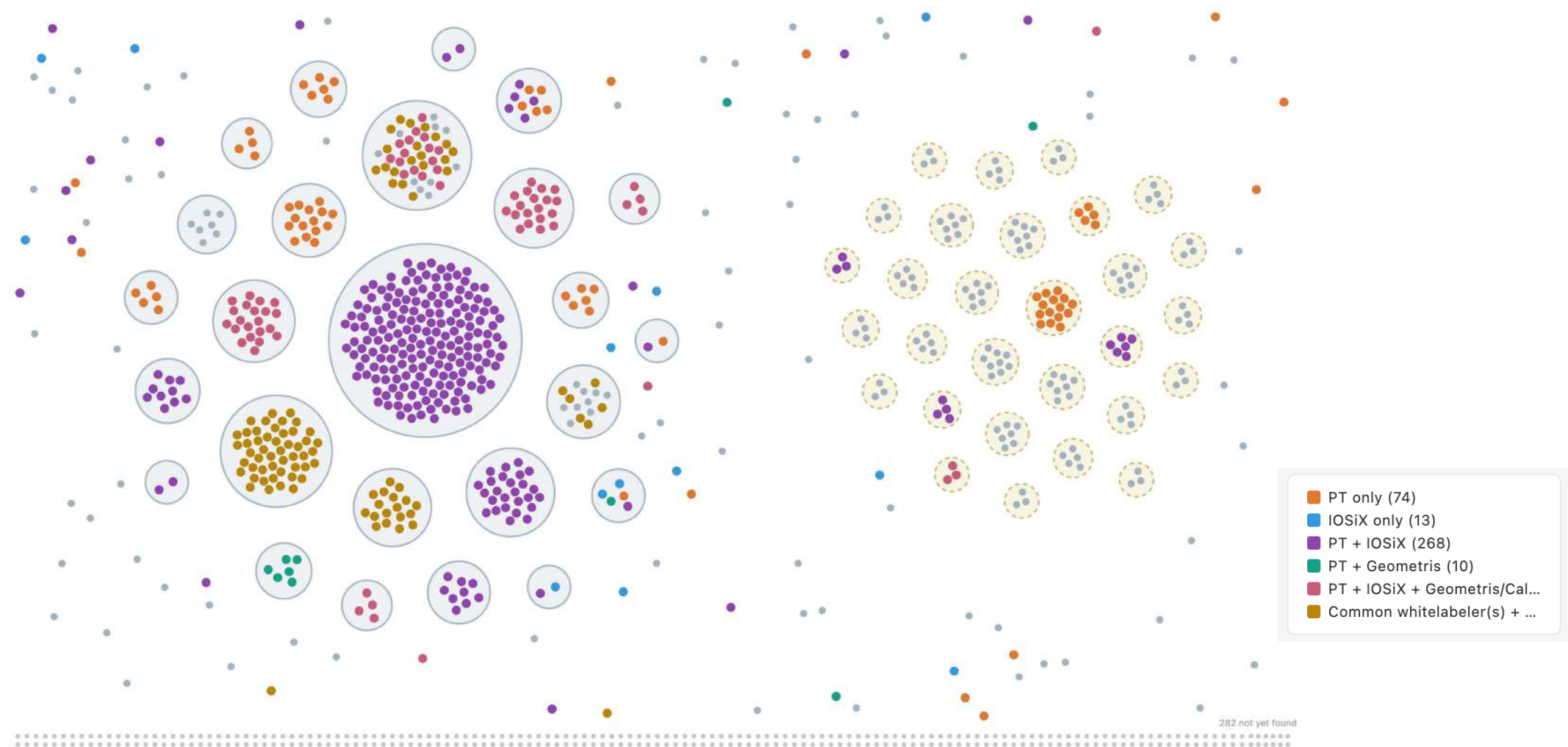
Hardware View: FMCSA Docs

ELD Hardware: Defined by FMCSA Docs



Hardware View: SDKs

ELD Hardware SDK



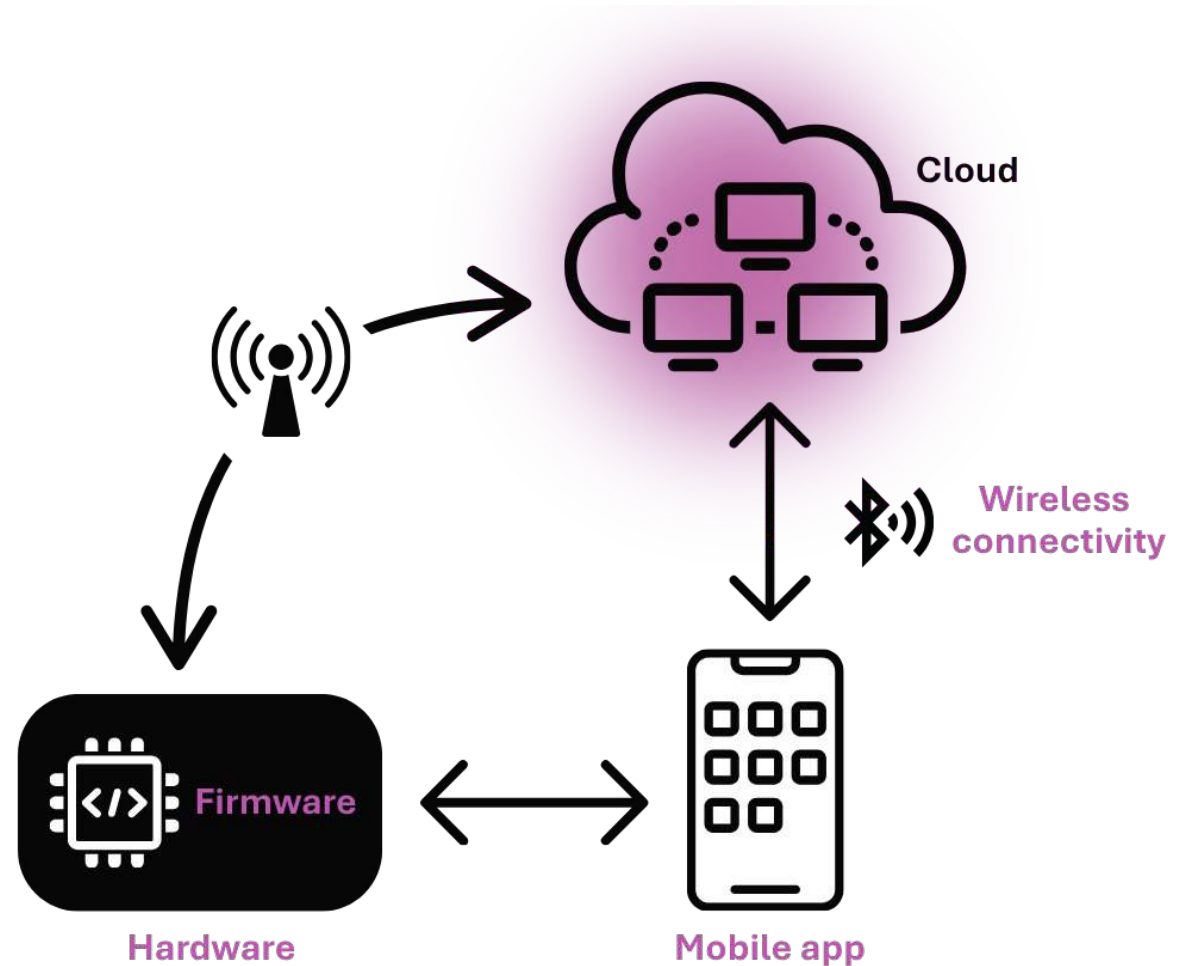
Cloud + 3rd Party

Shared risk questions:

- Are cloud assets shared?
- Are 3rd party integrations concentrating risk?

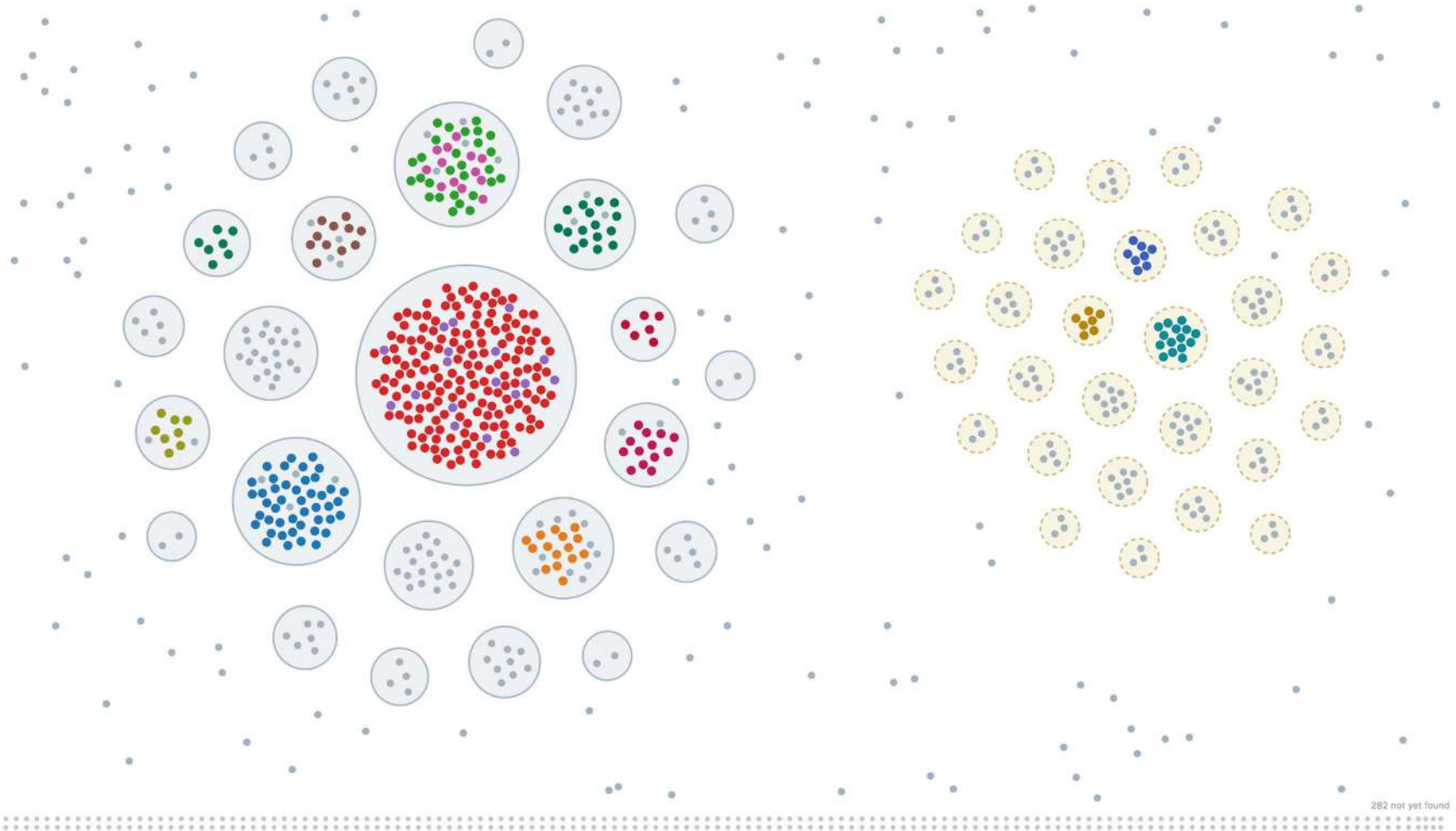
Why this matters:

- Cloud vulnerabilities = outsized impact
 - All customers can potentially be affected vs one-off hardware attacks
- Cloud infrastructure outages
- Biggest privacy and compliance risks



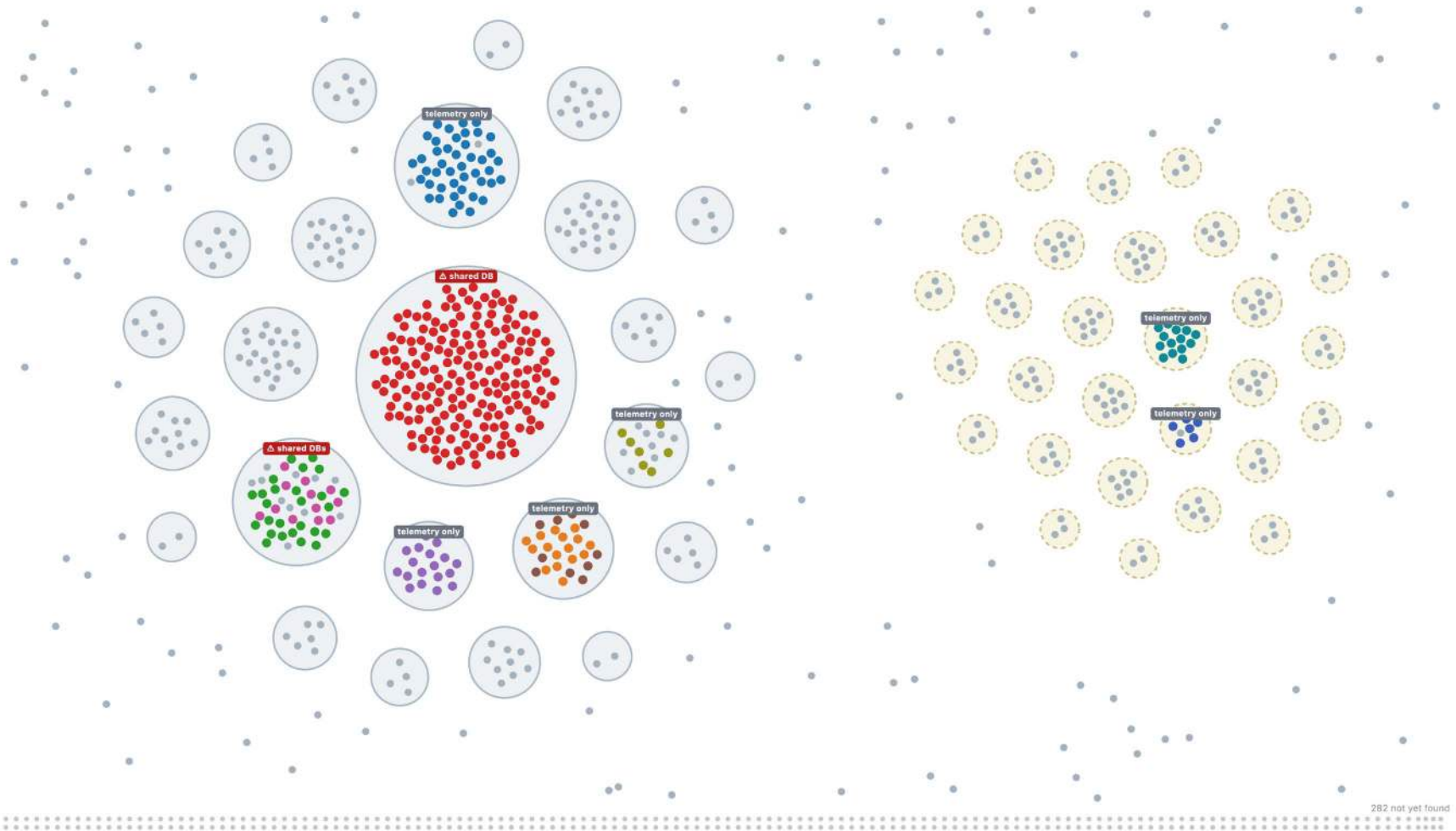
Shared APIs

Shared ELD Backend Servers (URL and IPs)



Shared 3rd Party (Hosted) Cloud Services

Shared ELD Cloud Services



Other Cloud Findings

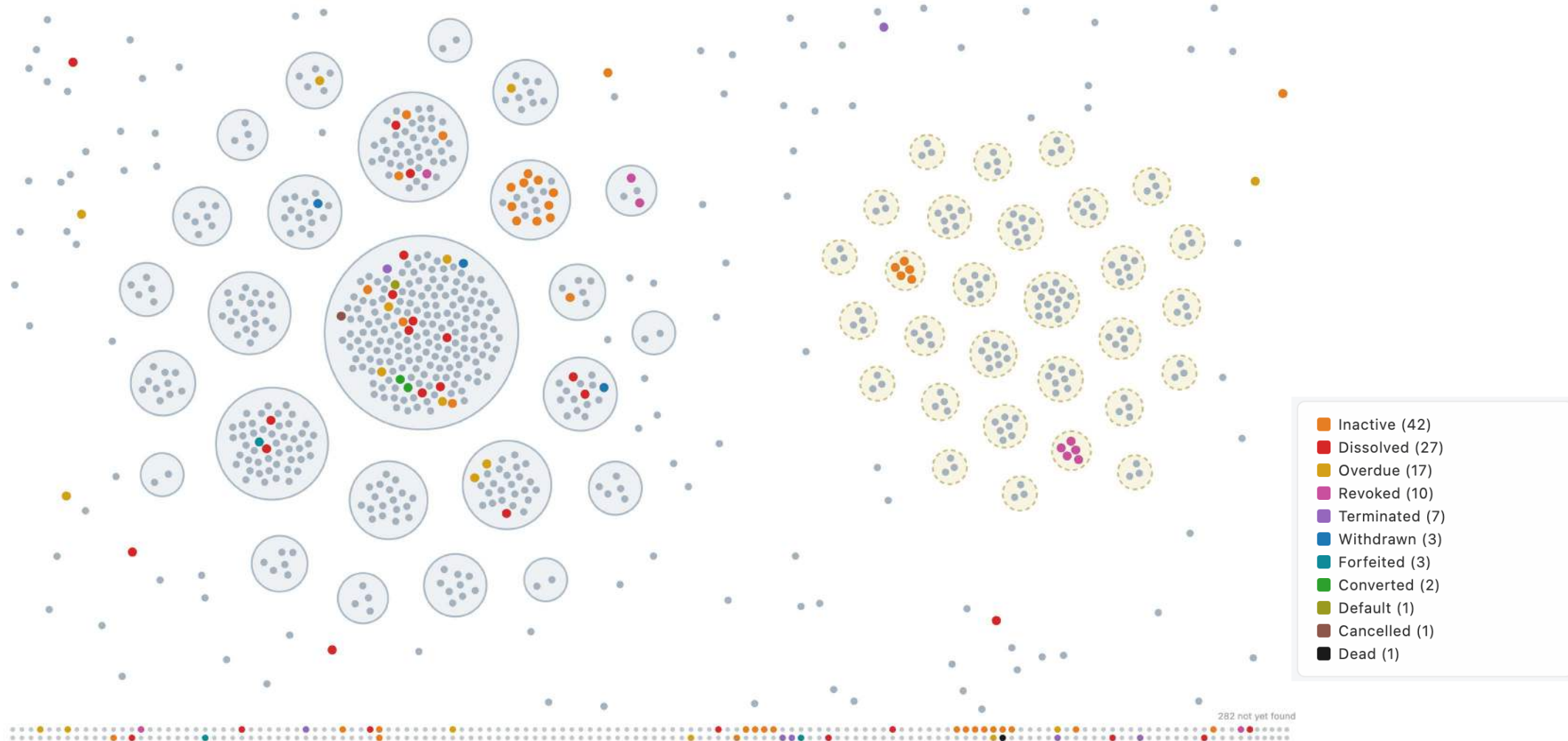
- IP lookups for all backend APIs to find server locations
- Some non-US/Canada companies host their data in the US/Canada
 - Server location not a useful proxy for foreign development
- Some apps use servers hosted at residential addresses
- ~50% using Cloudflare or WAF

Other Cloud Integrations

- Notifications
- Driver chat integrations (ex: dispatch)
- Geolocation services
- 3PL integrations
- AI analysis of driver behavior
- Stripe payments
- One app with a full internal social network (clone of Facebook)

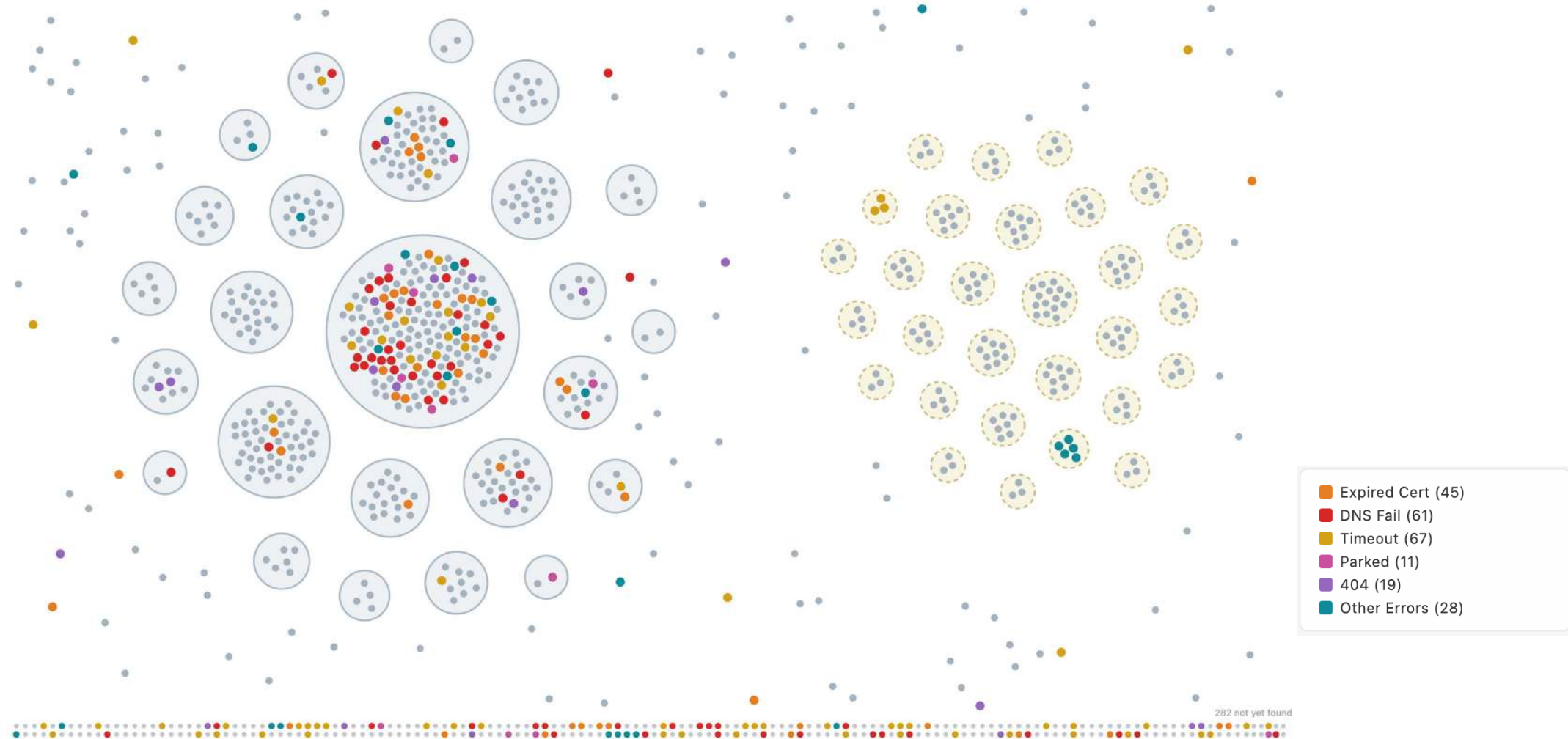
Defunct Companies?

ELD Company LLC Statuses



Defunct Companies?

ELD Website Statuses



Where Do We Go From Here?

- ~50% of ELDs by list count use white-labeled hardware
- ~75% of analyzed ELDs (by count) use white-labeled software
- Revocations hitting white-labeled families the hardest
- Families sharing databases and other cloud resources
- 10% of LLCs defunct, 20% of websites defunct

Where Do We Go From Here?

- Findings relevant to:
 - Trucking industry and NMFTA partners
 - FMCSA and other gov't agencies for regulatory reasons
 - Security researchers
- For carriers: NMFTA TSRM Resources and Questionnaire
- **Thank you to NMFTA and partners for support!**