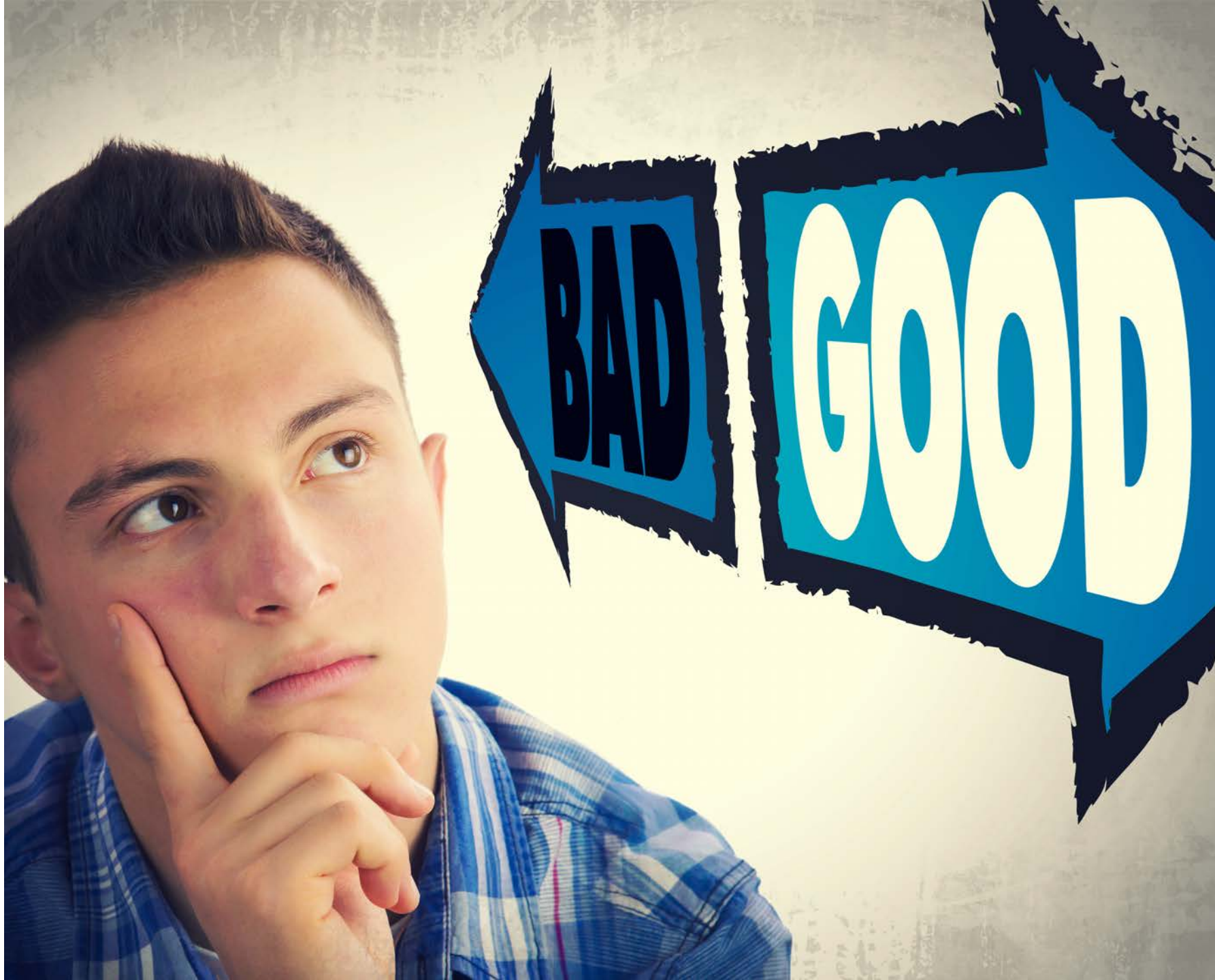
AppEsteem™

Certifying apps for a better world

Realizing the dream: how we'll get to a clean world

Dennis Batchelder
AppEsteem Corporation
June 2016

CSA Strategy: encourage vendors to be clean through self-regulation, safe havens…

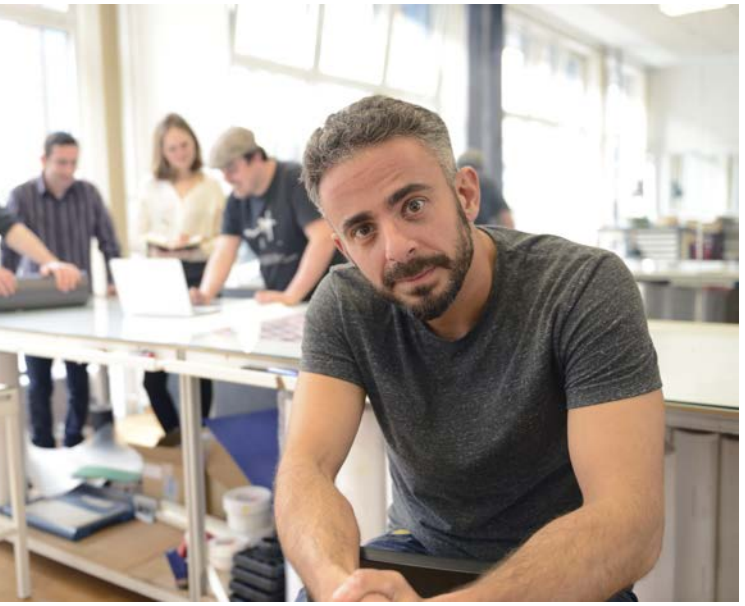


…and squeeze out the bad guys who keep screwing it all up

who fund their business by tricking customers

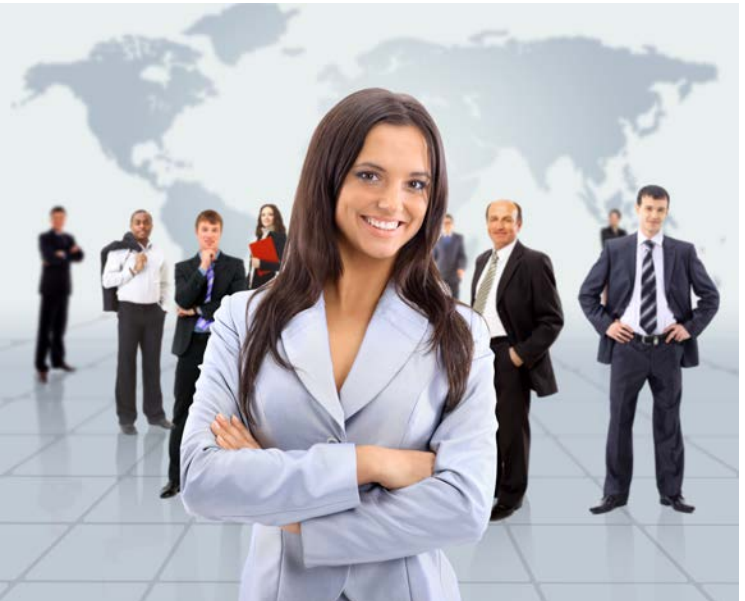
who grow their business by outbidding the good guys

Because a clean world is a better world

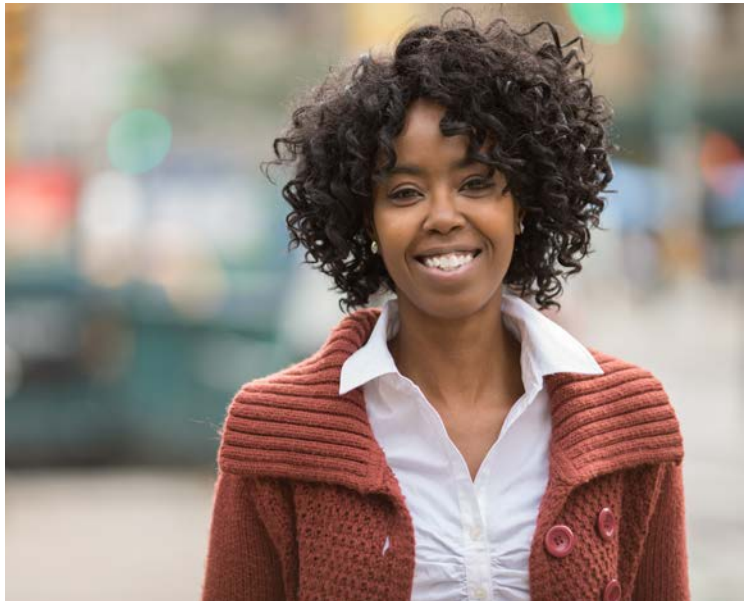


Independent software vendors build share, get paid, focus on value, thrive

Security vendors focus on getting rid of bad guys



Installers and download sites build brand value through clean exchanges



Customers install with confidence

But…we're still not there

We definitely have learned a lot

- These meetings are awesome
- Better communications, clearer guidelines, faster dispute resolution
- Some of the worst players quit

But we haven't operationalized

- Guidelines just now landing
- Membership and Governance still open
- Declaring you follow guidelines doesn't work

The monetization industry isn't clean

- The cleanest guys are abandoning the space
- Early supporters feel targeted
- We lack trust in each other

And consumers are still getting screwed ☹

My assertion: CSA only works with enforcement

AppEsteem will validate, certify, monitor, and enforce a clean app ecosystem

Validate vendors have good controls

- Advertising
- Customer data and complaints
- Partner selection and curation

Certify and “seal” apps

- CSA, Microsoft, Google guidelines
- Require built-in monitoring on every client

Monitor vendors and apps

- Build a true user sentiment story
- Suspend/remove as necessary

Share data to AVs and platforms

If you're a carrier, offer, installer, download manager:

Build your app

- ✓ Register your company and your product at AppEsteem
- ✓ Link your app with SRCL (pronounced "circle"), AppEsteem's self-regulating client library
- ✓ Use our portal to see free telemetry and analysis

Seal your app

- ✓ Get your company validated that you're using best practices to stay clean
- ✓ Submit your app for certification, and provide your distribution rules
- ✓ Your sealed app can be distributed by you and only the installers that you authorize
- ✓ Registered security companies and platforms can monitor any sealed app's behavior

You'll attest, we'll scrutinize, then we'll monitor

Pre-Certification analysis

Vendor disclosures and attestations

- Vendor attests to behavior
- Vendor to disclose trade names, certificates, download sites, reference creatives

Static and dynamic analysis in sandbox

- Build reference behavior graph
- Compute related apps/technology

Add reputation

- Website, app, certificates and interrelationships

AV detection information and history

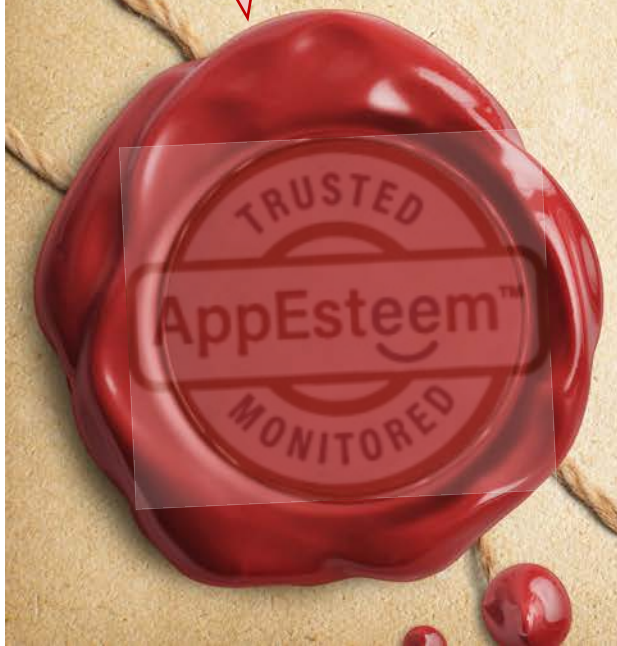
SRCL app monitoring

- ✓Malware heuristics
- ✓Behavior graph: processes, IPCs, files, registry, network
- ✓Distribution: source, packaging
- ✓Blocking/killing behavior (AV, platform)
- ✓Usage, Lifespan
- ✓Distribution violations

Inside the seal

1. Identification
   - Unique IDs and names
   - Dates
2. Distribution rights
   - Permitted and prohibited sites/parents/children
3. Certifications
   - Which guidelines the app meets (e.g., CSA, Microsoft, Google)
4. Vendor attestations
   - Statements by vendor on the app's value and how it monetizes
5. Signature
   - File/Seal fast/full hashes, AppEsteem cert

1) Vendor signs app, submits
2) AppEsteem certifies and builds seal
3) Vendor packages seal, re-signs app
4) AppEsteem registers app



Identification	Seal ID Grant/Expire Dates App Name, ID, Version Vendor Name, Id Signing Certificate Thumbprint
Distribution Rights	W3C's ORDL-JSON format
Certifications	Guidelines/version numbers (URL)
Attestations	Value statement Monetization statement
Signature	Digital signatures in XML-DigSig/XAdES format with timestamping for fast and full validation

If you're an AV, Platform, you'll also monitor

AppEsteem security partners will:

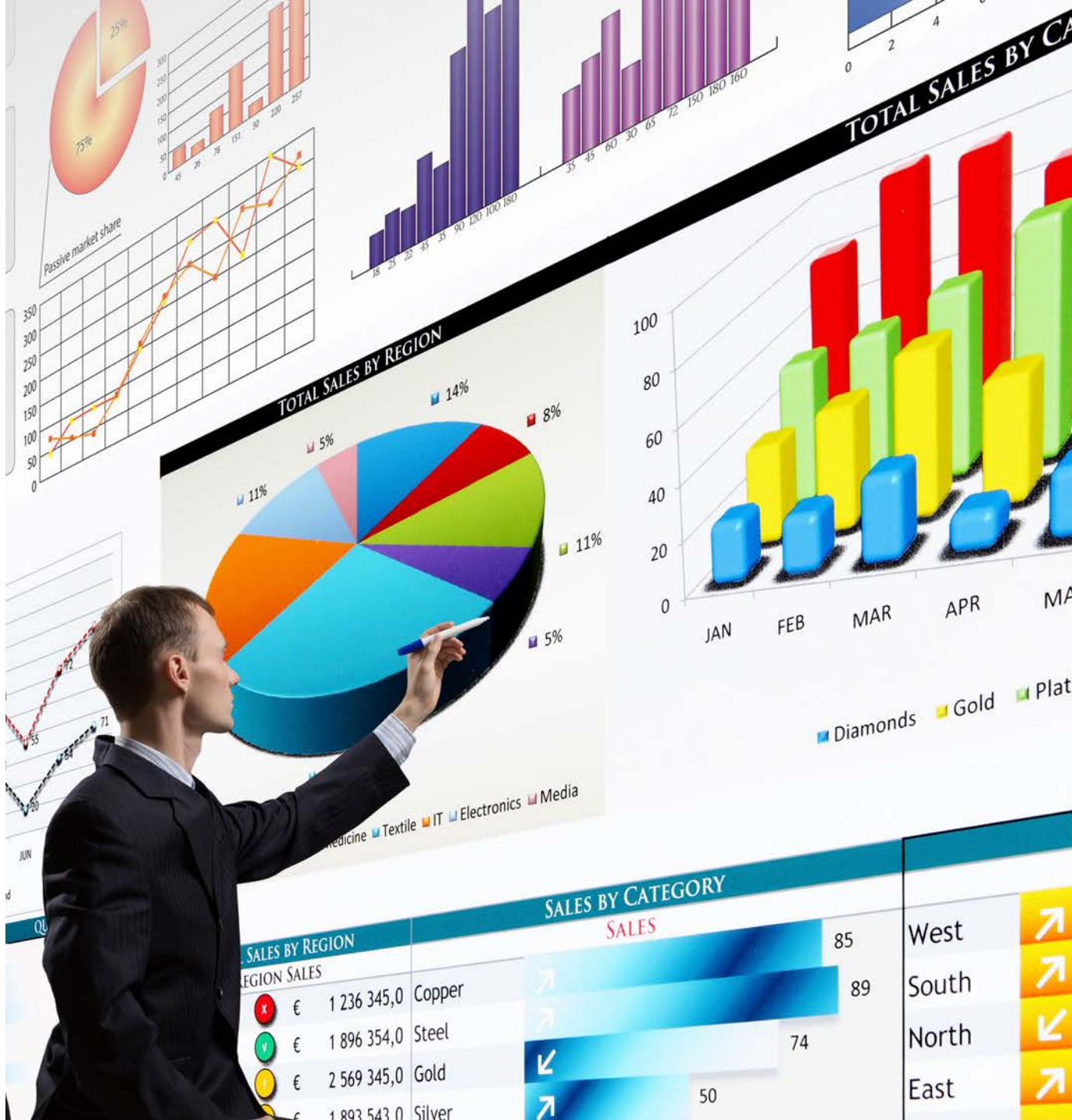
- Validate seals
- Help enforce distribution
- Let AppEsteem handle issue resolution

And get online app intelligence

- Vendor relationships
- App history, related seals
- Observed behavior graphs
- Distribution summaries
- AV detection history
- Online status checks

As well as cache downloads

- Trusted Vendor and App Ids
- Seal revocations
- App and vendor suspensions



The road to Beta

April - June: Done

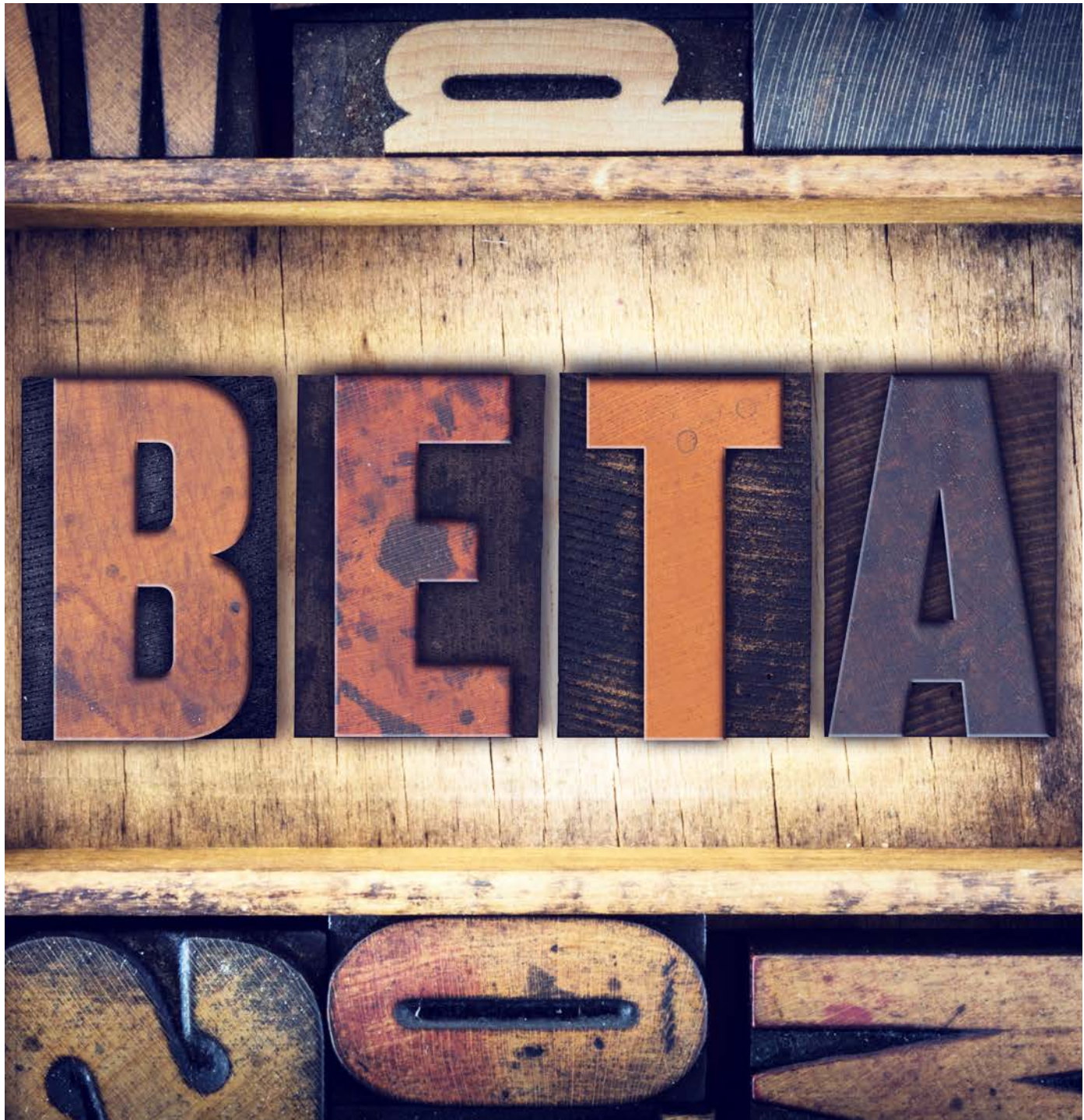
- ✓ Road show with AVs, platforms, CSA, Compliance officers
- ✓ Recruit dev/research team
- ✓ Sign up installers/downloaders
  - ✓ Tightrope, AirInstaller
- ✓ Figure out monetization plan

Still in progress…

- Land MOU with CSA
- Help CSA finalize guidelines, membership, governance, fees
- Establish validation and certification scorecards
- Deliver first cut of SRCL and seals
- Sign up carriers, offers
- Get more AVs into beta

July - September: run betas

- Goal: 1 installer, 2 download sites, 2 carriers, <10 advertisers
- Windows PE (July) CRX (September)



What the beta will measure

Can we increase customer offer satisfaction?	Can we reduce vendor evasion?
***Hypothesis**: Offer screens trick customers to clicking through and leave them dissatisfied. Sealed apps with certified offer screens will lead to better informed and happier customers.*	***Hypothesis**: Today's installers evade detection by morphing hosting locations, digital signatures, product updates, brand names, and domains. Sealed apps won't need this, which reduces the cost to protect*
Measuring success Reduced sealed offer startup rates. Increase sealed app lifetime	**Measuring success** Less evasion: reduced certificates, domains, landing pages, product updates for sealed offers

What it means to be in the beta

Participate in weekly planning/operation calls

- Land the seal design/integration
- Influence what data will be provided
- Help devise a workable issue resolution system

Vendors get validated and certified

- Disclosures, controls, attestations, apps

AVs/Platforms sign off on validations and apps, receiving monitoring data

We measure, learn, pivot as necessary

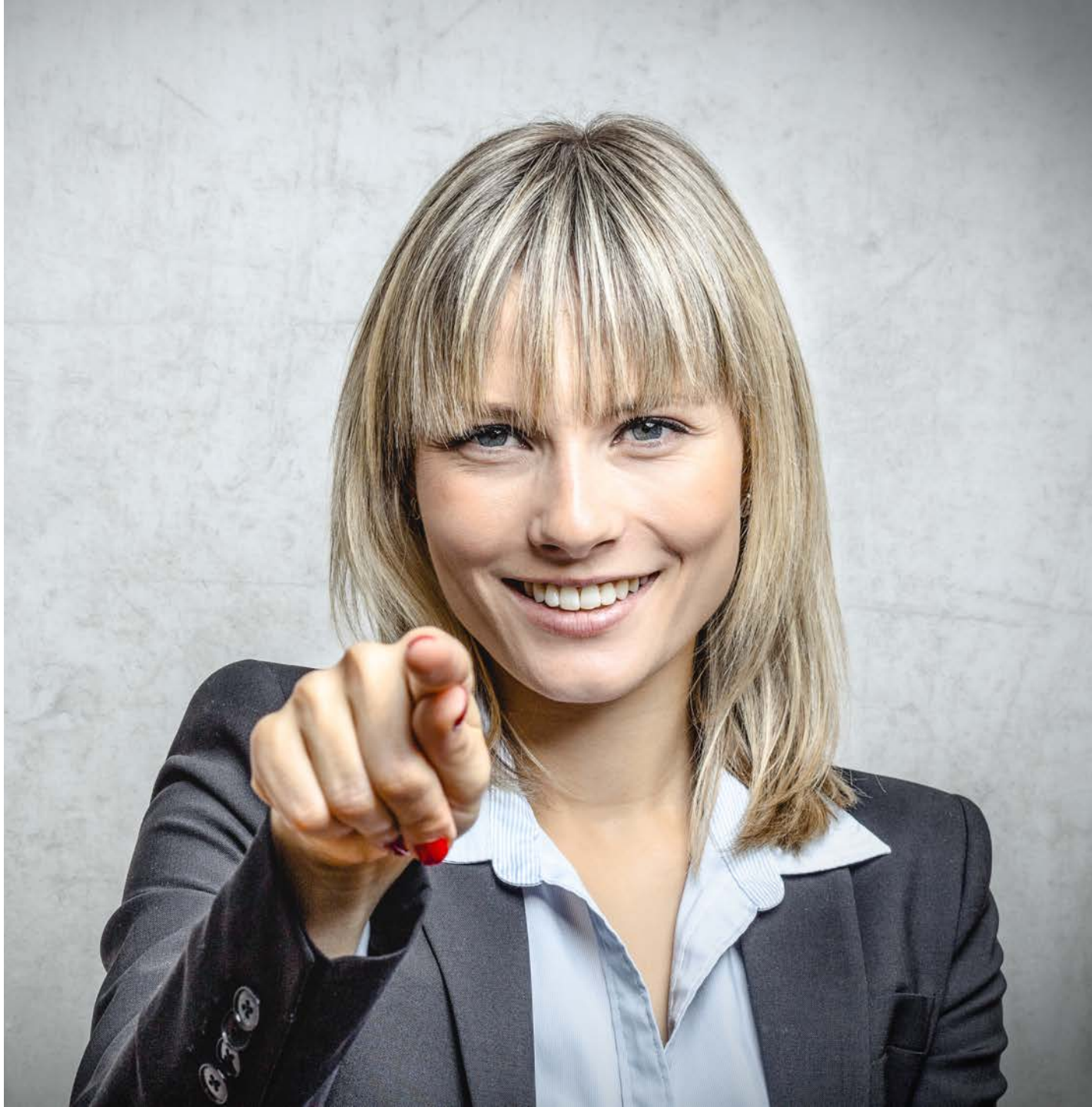
We want you to join the beta!

AVs/Platforms: let me know

Carriers/Offers: talk to Tightrope and RedBrick

Remember:

- EXEs first (July)
- CRXs next (September)



Some food for thought

We need CSA:

- Regulations: unless we're happy with non-consumer-focused guidelines
- Unity: Working together does drive change

You need to be serious about cleaning up

- AVs and platforms only willing because they can get tougher on those who don't seal
- It means we have to monitor ourselves

If you do, it can be profitable and stable

- There's latent demand from high-quality carriers and offers
- With no race to the bottom, prices won't be insane with crazy fluctuations

But it's going to take courage

- It's hard to change, especially when you're asked to be first

And it will still be a bumpy ride

- Until we cover EXEs, CRXs, APTs
- Until the whole supply chain is sealed
- Until we reach critical mass

AppEsteem™

Certifying apps for a better world

http://appesteem.com
info@appesteem.com
@appesteem