Near-death experience

Why AVs get clobbered by unwanted software (and how they'll win)

Dennis Batchelder
AppEsteem Corporation
AVAR 2016 (Malaysia)

Software monetizers are businesses

- They make millions in revenue
- They are proud of their brands
- They use sophisticated direct marketing and A/B testing to maximize their consumer “conversions”
- Most security partners are also software monetizers
  - Scan/try/buy and freemium models
  - Offer other products/services
  - Pay per install with other carriers
  - Pay per install with new PCs
  - Alternative monetization: display ads, safe search, ad blocking, price comparisons

Software monetization becomes unwanted when…

- … consumers are **tricked** into giving consent (or not even asked)
- … consumers are **unpleasantly surprised** by what did (or didn't) happen
- … consumers **feel cheated** by what they paid for

This industry has many opportunities for consumer abuse

- Aggressive and unauthorized affiliates
- Displaying scary and lying ads
- Misleading and tricky landing pages
- Installing without consent
- Annoying and scaring with ads and warnings
- Up-selling and cross-selling during payment and support

The vendor perspective

- They admit they’re being aggressive
- They claim lack of clarity on detections
- They see many conflicts of interest by the “protectors”
  - Platforms are aggressive with updates, changing defaults, collecting telemetry
  - AVs seen as scaring consumers during trials to upsell
  - AVs sell system tools and their detections look like they’re blocking competitors
  - Browsers and platforms look like they’re protecting their own monetization
- … so they morph and evade and call their lawyers
  - New brands, companies, landing pages, certificates, advertisements, web-configured behavior

Result: AVs fail to protect from unwanted software

- Automation fails
  - Hard to actuate and replicate
- Behavior monitoring fails
  - Apps obtain user consent, use normal distribution
- Malware analysis fails
  - Landing pages, brands, docs, advertising, up-selling need checking; change rapidly
- Human response fails
  - Software vendors fight back with lawyers, not evasion
  - Policing external behavior isn't what researchers signed up for
- Testing fails
  - Comparative testers are slow to enter this space

If an AV cannot protect its consumers from unwanted software, its future looks **bleak**

We’ve been solving this problem together for almost three years

- 2014: Microsoft pushes for a new approach
  - Formation meetings in Israel, Florida, Canterbury
- 2015-2016: Clean Software Alliance picks up steam
  - Summits in Vegas, NYC, Prague, California
  - Publish software and advertising guidelines
- 2016: AppEsteem starts certifying apps
  - Published broad app cert requirements
  - Defined monitoring for apps, landing pages, and better world network partners
  - Agreed that CSA will provide oversight
  - Launched pilot

The premise:

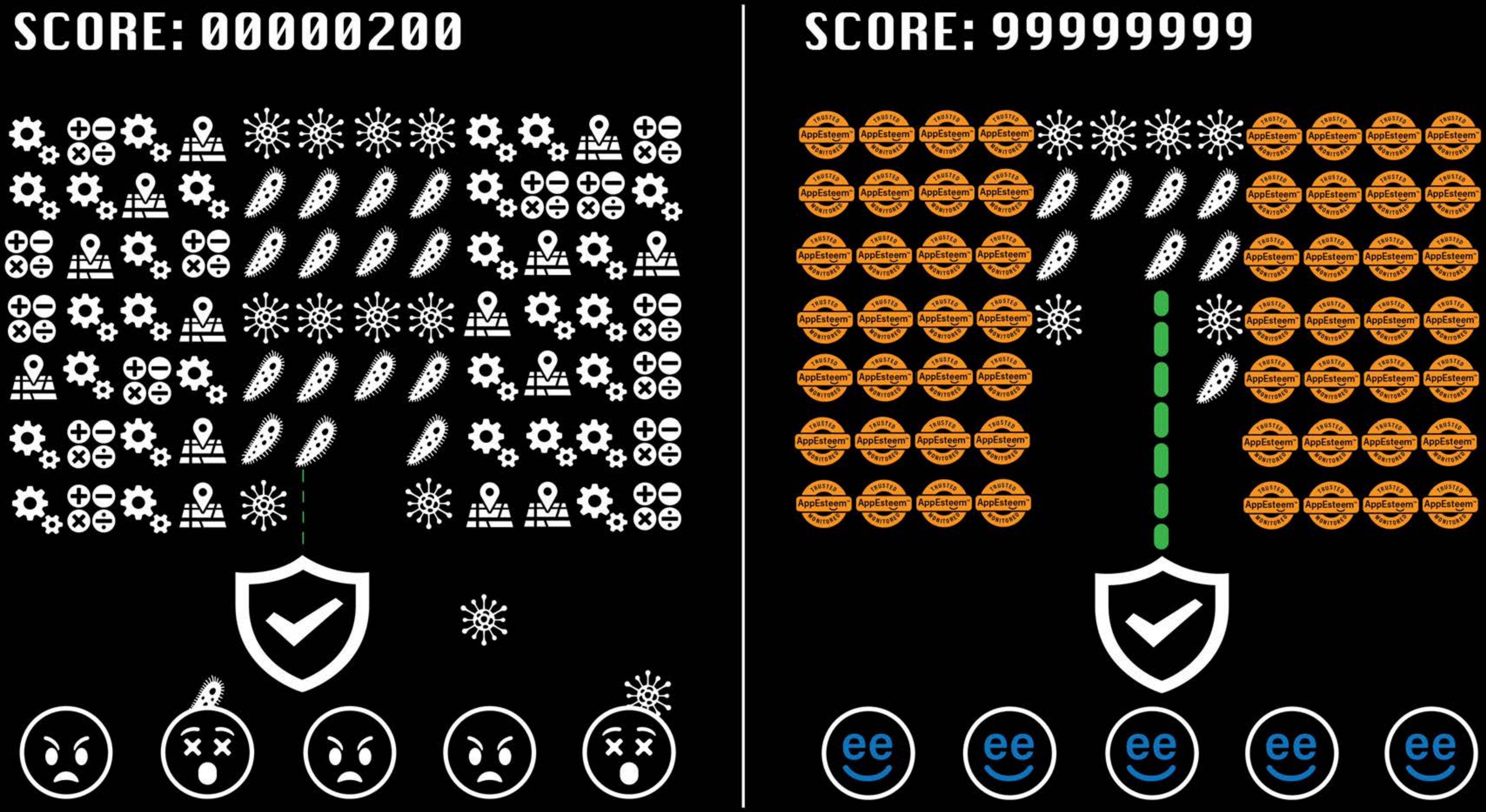
If we provide a safe haven for clean apps…

…we can get much more aggressive and squeeze out the dirty apps

who fund their business by tricking and cheating customers

who grow their business by outbidding the clean players

Certification drives vendor change and helps AVs succeed



Before AppEsteem

Certified apps make a better world

AppEsteem's pilot launched last month

- 21 Security partners (not all committed; some watching)
- 5 Software monetization vendors (18 more in pipeline)
- 5 Better World Network partners
  - Compliance officers, payment processors, call centers, AV monitoring services
  - Planning to add ad networks, downloaders
- Overseen by the Clean Software Alliance

- Manual stage (Nov-Dec 2016)
  - Validate the requirements
  - Set up communication paths
  - Train certifiers
- Automated stage (Jan-Mar 2017)
  - SRCL monitoring/reporting
  - Automated sigs and online verification
  - Embedded seal/taggant

Certification indeed led to vendors changing their apps

Product Category	Example area changed for certification
Web Browser	Software: Misleading icons, hidden browser popup, app doesn’t close
New Tab (Chrome Extension)	Interstitial offer: didn’t close, over-integrated into carrier flow and not clearly separable
PC Optimizer tool	Call center: aggressive upselling of tech support
PC Optimizer tool	Call to action/payment: needed to highlight the need to pay before fixing
PC Optimizer tool	Install: hidden component not disclosed, not un-installable

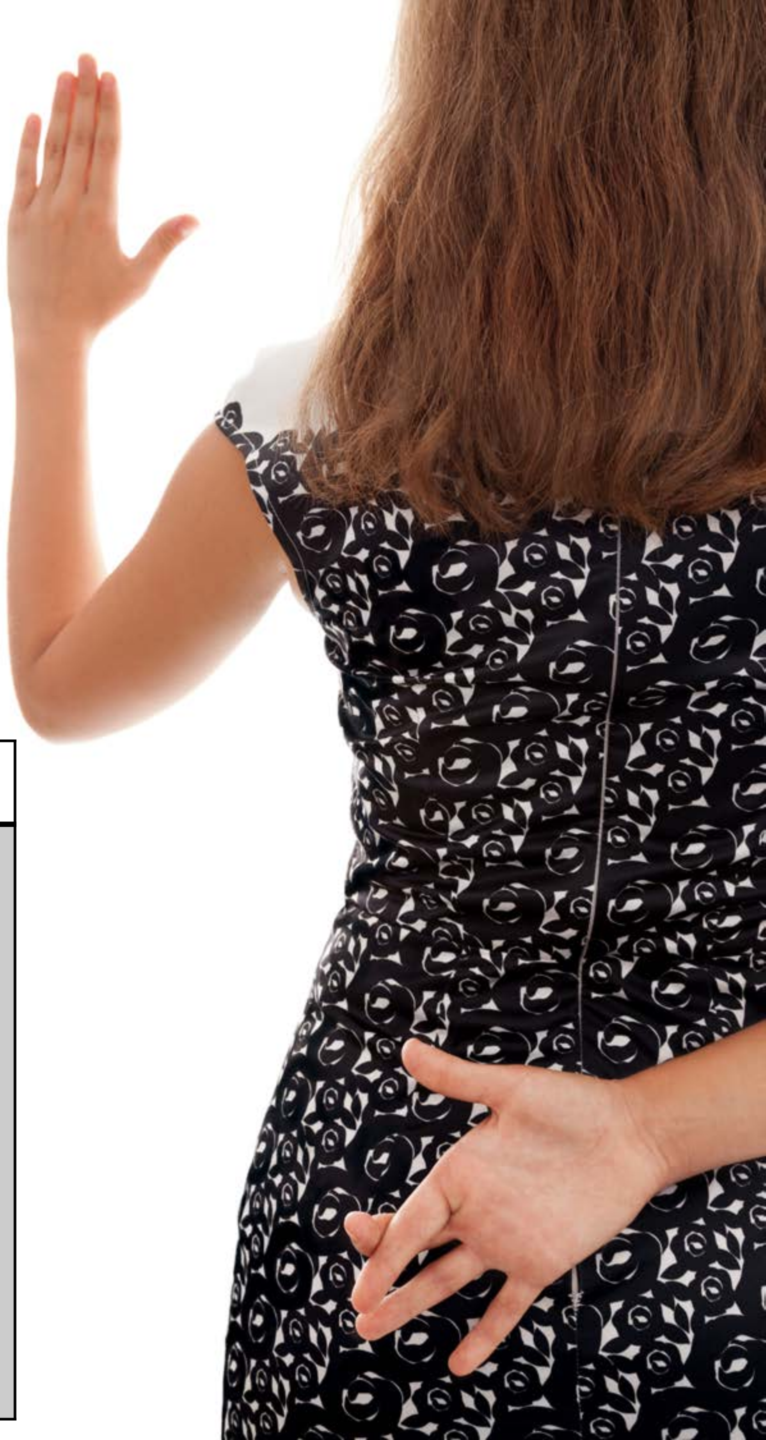
What we’ve learned from our Security Partners

- We missed/needed clarification on requirements and disclosures
  - Call centers, target OS/browsers, distinct clean certificates and dev accounts
- It takes time to trust AppEsteem
  - Especially when partner doesn’t know us
  - Areas of difficulty: perceived conflict of interest; fear of trusting or rewarding the “bad guys”
  - Our response: we collect for monitoring; we need to create an alternative path
- It takes time for our partners to change client and cloud code
  - Today partners are whitelisting and are waiting for our tech
- Security partner apps have their own issues
  - But it’s important to be consistent
  - We’re looking for ways to accelerate the cleanup

What we’ve learned from Software Vendors

- Many vendors are mature enough to take the leap
- Few want to be monitored; few are happy to pay
- Detections drive urgency, but vendor still has to “convert” their culture
- We spent too much time with those not ready to convert, who seem to want it both ways

Signals of culture conversion	Signals of unsuccessful culture conversion
• Finding ways to measure and respond to consumer sentiment • Killing apps that have no intrinsic value • Moving to cleaner affiliates, call centers (or shutting them down) • Shifting to a long-term payment relationship with consumers • Seeking to understand the intentions behind the requirements	• Too-fast, unquestioning submission of contracts, attestations • Loud protestations of “we’re so clean”, “nobody detects us” • Looking for ways to get around monitoring and certification • Withdrawing/substituting apps • Offering to pay extra to make the problem go away



Consumers need you to get this right

- Join the pilot
  - Win the fight against unwanted software
  - Help us nail the requirements
  - Reduce your work
  - Reduce your risk
- Use the requirements
  - They’re free, and they’re great
- Commit to keeping your own apps clean
  - We can’t afford to be hypocrites
  - It’ll help in future tests

AppEsteem™

Certifying apps for a better world

https://appesteem.com
@appesteem

Review our docs and sign up:	https://appesteem.com/documents.html
App certification requirements:	https://customer.appesteem.com/Home/AppCertReqs