Vision and Plan

Our Vision

Consumers have nothing to fear when installing and using free apps on their computing devices.

Our Mission

AppEsteem provides the technology and services necessary for the software monetization industry to self-regulate, clean up its act, and thrive.

The shape of the software monetization industry

Software monetization is how software vendors use the power of "free" along with alternative monetization approaches to achieve app distribution.

There are many moving parts in the software monetization space:

1) The **consumer**, who seeks out or is enticed to install a desirable app.
2) The **software vendor** who builds that app, called a **carrier app**. These vendors give away the app for "free", and monetize by including offers at install time, displaying advertising, cross-selling other related products, and offering in-app purchases and upsell opportunities to consumers.
3) Getting web **traffic** for distribution
    a. The carrier app is available for download from the app's **landing page**. The software vendor typically buys media (advertising) to bring consumers (web traffic) to this landing page.
    b. The carrier app may also be listed on a **download site**, which may list many apps available for consumers to download.
    c. The software vendor and the download site may use **affiliates**, paying them when the traffic they bring to the landing pages and download sites results in user installs.
4) **Bundlers**: the carrier app may be bundled with other software offers. This happens mostly with Windows non-store apps listed on download sites.
    a. The bundler builds an **installer** for the carrier app that may contain a search offer and one or more software offers. The carrier app may be embedded inside the installer along with the offers, or the installer may be a **download manager** that downloads the individual software on demand. Bundlers create marketplaces between the carrier apps and the offers.
    b. The installer may make a **search offer** to change the default search provider (through default settings, extensions, and toolbars) on the computing device of the consumer installing the carrier app.
    c. The software vendors who build the **software offers**, and are willing to pay to be installed on the consumer's computing device, because they have a post-install monetization strategy (examples include antimalware products, Chrome extensions, ad injectors, ad-supported products, and other value-added services), and they're looking for more distribution.
5) The carrier app and the software offers may monetize by displaying ads either in their product, in the browser, or on the platform. They become affiliates of **advertising syndicators** to get relevant ads.
6) The **platforms**, the operating systems, stores, browsers, and exchanges, who wish to control ads, search, apps, and software on behalf of consumers.
7) The **antimalware vendors**, who try to prevent malicious and unwanted software from disturbing the consumer.

Note that the model described is simple, but in reality, the relationship between the players is also recursive and incestuous: a software offer inside of a bundle may bring along its own monetization, in which case it's acting as a carrier app. Other examples: bundlers may provide their own carriers and offers, offers may be sold without carriers, and Chrome extensions may include their own search offer.

In the ideal world…

When this ecosystem works properly, here's what happens:

1) The consumer understands and consents, is not unpleasantly surprised, and doesn't feel cheated by the carrier app, the way he was led to it, and the monetization it uses.
2) The bundler, carrier app, offers, and advertising syndicates are able to monitor for and remedy fraudulent behavior from each other and their affiliates.
3) The installed apps and search offers respect the boundaries set by the platforms and antimalware vendors.
4) All players are competing fairly, assured that clean behavior outperforms fraudulent behavior.

A tragedy of the commons

Unfortunately, this ideal world does not exist, because the software monetization industry leaves many opportunities for bad players to surprise and cheat consumers and commit fraud against each other. Some examples:

1) Affiliates
    a. Trick and scare consumers with false advertising
    b. Use click-fraud, false impressions, and hijacked identities to drive web traffic/installs
2) Bundlers
    a. Drive high offer conversions with tricky offer screens
    b. Offer fake or unlicensed/unauthorized carrier apps
    c. Evade security software detections using tactics employed by malware authors
3) Download sites
    a. May buy SEM to divert traffic from official carrier apps to their unauthorized or nonfunctioning bundles
4) Carrier apps, search affiliates, and software offers
    a. Act differently/break the bundler rules post-install
    b. Stray out of bounds of the platform rules (defaults, advertising)
    c. Overwhelm consumers with unrelated, annoying, or overwritten advertising
5) Advertising Syndicates
    a. Provide unrelated, malicious, and unwanted ads
6) Platforms and antimalware vendors
    a. Take advantage of their privileged position to flout the rules they enforce on others

The industry's use of unregulated affiliate networks and auction-style marketplaces gives advantages to ruthless and unscrupulous players. It is difficult for the bundlers, advertisers, and software vendors to validate and regulate each other and their affiliates. Because fraudulent approaches pay well, bad players are able to out-bid others, and the incentives to fix the problem are lacking.

It's a vicious cycle: Aggressive distribution approaches may lead to higher revenues, but they also bring higher consumer complaints. The complaints cause antimalware vendors and platforms to add friction to installs and issue ever-stricter guidelines on what isn't allowed. This drives the industry toward increased evasion, even more aggressive behavior, and a loss of opportunity for those trying to follow the responsible guidelines.

What results is a tragedy of the commons: because of a lack of self-control inside the various affiliate programs, the software monetization industry is destroying its supply. Industry players now shift to maximize the short-term only, because of the pervasive belief that it will soon collapse.

The largest sufferers of all are the consumers: overwhelmed with bad apps on their computing devices, they are losing faith in independent software vendors and in the platforms.

So why not let it implode?

A great question to ask is whether it makes sense to let the software monetization industry collapse and be replaced by app stores run by the platforms. In a world where platforms have the power to not only block apps from their stores, but remove pre-installed apps, it's true that there seems to be less room for fraud. But in reality, these systems have significant gaps that are getting exploited. We see this in both Apple's App Store and Google's Play:

1) Down-level and alternatives are pervasive: Windows has years before its legacy non-store apps disappear in Windows 10, and over a billion consumers use non-store-enabled versions of Windows. Google Play isn't pervasive or required. It's not even allowed in China, where hundreds of millions of consumers use alternative, unregulated stores to get their apps. Apple's App Store allows profiles, which are exploited by fraudulent players to side-load bad apps.
2) Monetization still exists: Apps on all platforms still monetize with in-app and other advertising, and fraud here still brings consumers grief.
3) Doesn't address traffic: false advertising and fraudulent affiliates driving web traffic to "safe" stores still leave consumers unpleasantly surprised and feeling cheated.

Whether software is independently downloadable or store-based, a better-regulated software monetization industry would enable independent software vendors and the supporting ecosystem to flourish. Consumers would benefit from additional choice and innovation. The platforms would benefit from happier consumers freed from the worry of getting into unwanted situations.

What has been tried

The Clean Software Alliance (CSA) was established as a means for the software monetization industry to self-regulate, allowing the compliant players to flourish and even get rewarded while the antimalware vendors and platform focus their blocking efforts against the non-compliant. A proposed final set of guidelines has been established. But these guidelines don't address advertising or system tools, and they've been neither operationalized nor enforced by CSA. It's easy for vendors to claim that they are compliant with nobody to validate their claims, or to certify and monitor their apps. This degrades the value of the guidelines, and the value of the claims to be clean.

Beyond the scope of CSA, each browser and store and security player continues to set their own guidelines as they attempt to keep consumers safe from the bad players in the software monetization industry. These multiple and sometimes contradictory guidelines, which continue to change as the industry evades, put pressure on the software vendors, advertisers, and bundlers to ensure they meet the guidelines.

The platforms and antimalware vendors try to sort out what's clean and what's not, and they do this through manual and automated analysis. The cost of evaluating each version in labs without the participation of the software vendors is both expensive and risky for each vendor; if they get their certification wrong, they may be sued.

There is a need for an independent certifier to help those in the software monetization industry who desire to play by the rules. There is need for a structure that lets these "good" players band together as a collective in a way that the platforms and antimalware products would be willing to either get tougher against bad players or offer benefits for the good players. There is a need from the platforms and antimalware vendors to have a trusted authority who monitors the software monetization players and whether their software complies with the policies.

The role of AppEsteem

AppEsteem plans to offer services to enable the "good" software monetization industry vendors to take back the industry and operate in an ecosystem isolated from the bad players. The services include:

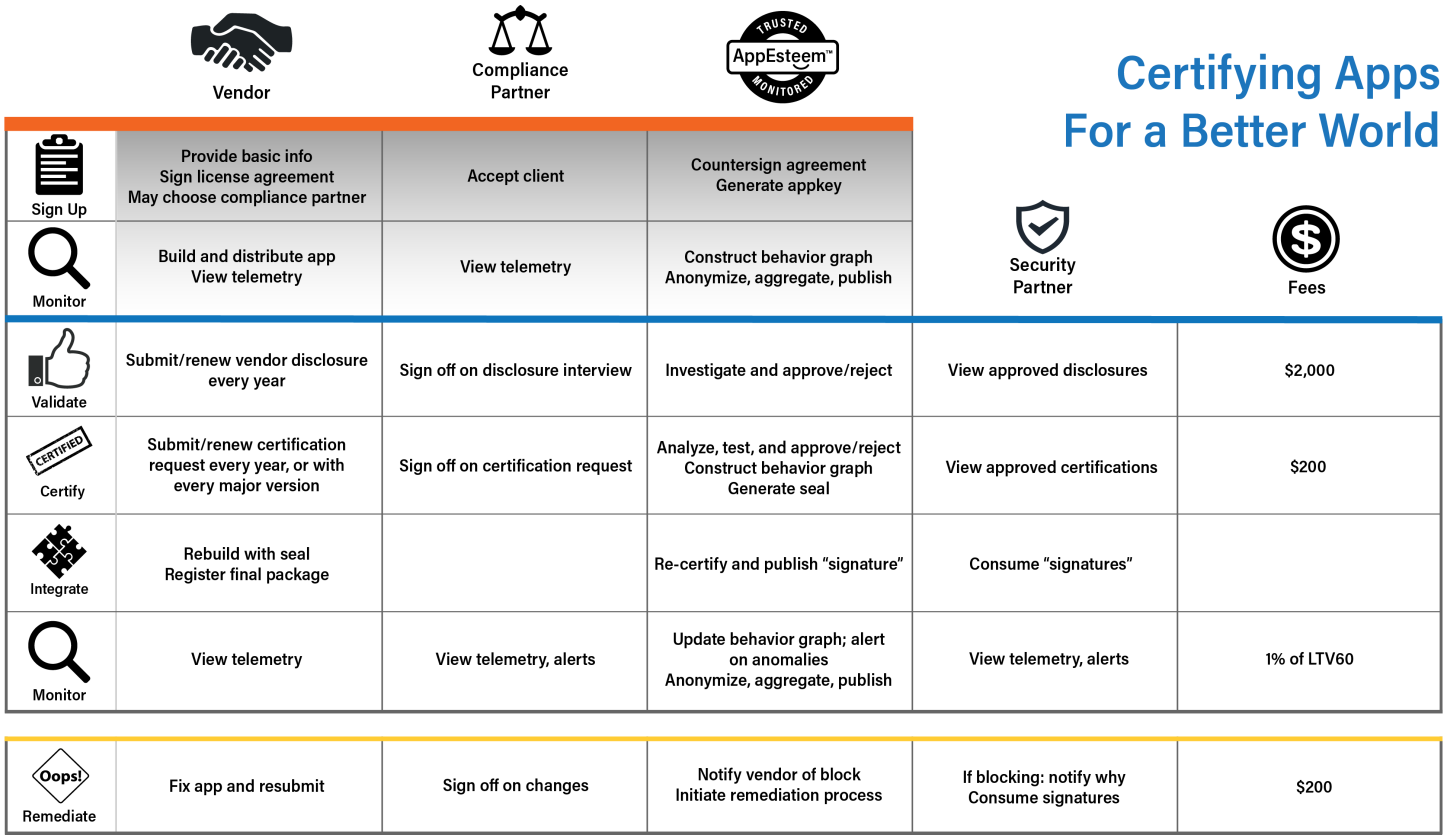
1) To software vendors and bundlers: Certification and monitoring of the apps. Enforcement of distribution policies. App intelligence to help grow an app's esteem by its consumers. A set of trusted business partners that reduces costs. Support against fraudulent competitors.
2) To service providers: business opportunities inside a clean, self-regulated ecosystem with less risk of fraudulent behavior.
3) To antimalware vendors and platforms: Access to certified app disclosures and telemetry.

These services provide benefits to the industry players:

1) Consumers will be able to trust sealed apps: their advertisements, their landing pages, their value claims, and their behavior.
2) Carrier apps, software offers, and bundlers can spend less time managing fraud and evading detection, and more time delivering consumer value. They will have a channel for dispute and resolution, a trusted set of business partners that don't treat them with suspicion, and assurance that fraudulent competitors will be held accountable for their actions.
3) Antimalware vendors and platforms will be able to focus more of their efforts on the truly bad software, and less on those trying to follow the rules. This includes the time they'll save by having AppEsteem handle a dispute and resolution verification process for the vendors.
4) Platforms benefit by having happier consumers.

Scenario and Monetization Overview

The diagram shows the typical flow of how software vendors, compliance partners, and security partners interact with AppEsteem. All fees shown in this flow are paid by the software vendors.



Our Scenarios

Building the app

A software vendor is building a new app, and wants to use AppEsteem's monitoring library. They will do the following:

1) Register with AppEsteem to use a free compliance-monitoring library that gets compiled/linked/loaded into their app
2) Learn insights about their product distribution and whether it's getting blocked

Sealing the apps

The installer, download manager, carrier app, and software offers all need to be certified. They will do the following:

1) Ensure the app is compliant with CSA, Microsoft, Google, and AppEsteem's guidelines
2) Disclose company information and attest to controls to be validated
3) Disclose app information to AppEsteem for certification
    a. Define distribution constraints and entitlements for this version of the app
    b. AppEsteem "seals" the app with a unique identifier as well as basic information of certifications, categories, and constraints

At install

At the time of the install:

1) The platform may give special friction-reducing benefits and promotions to AppEsteem-sealed software (either directly or indirectly by making it harder for non-sealed apps to install)
2) The anti-malware software validates the install executable as well as the individual software and offers are sealed appropriately by calling a free interface
3) As the software installs, the AppEsteem library self-enforces the distribution constraints and entitlements of each offer
4) Each sealed app sends back monitoring telemetry to AppEsteem

Monitoring (AppEsteem will provide a freemium model for these services)

1) If they're using AppEsteem's monitoring library, software vendors can monitor their app performance, fraud, distribution, and blocking actions (for both sealed and non-sealed apps)
2) Security partners (antimalware vendors and platforms) can monitor app distribution as well as app and vendor reputation and potential FNs/FPs (for AppEsteem-sealed apps only)

Our Monetization

AppEsteem will charge company validation and application certification on a transactional basis. The validations and certifications last a single year, which will drive a regular revenue stream.

We plan to charge the following to software vendors:

1) $2,000 for annual company validations (less $500 if company uses a trusted compliance officer)
2) $200 for annual app certifications (less $50 if company uses a trusted compliance officer)
3) Monitoring fee for sealed apps
    a. 1% of LTV60 charged to bundlers, download sites, software vendors, and trusted ad syndicators. We will charge bundlers and ad syndicators where necessary, or it would help simplify handling and add additional monitoring (includes ad/offer revenues and carrier app payouts)
    b. 1% of LTV60 charged directly to software vendors for direct downloads and inline installs (LTV60)

The principles behind our fee structure:

1) Keep the transactional fees low
2) Align AppEsteem's success with the success of the software monetization industry: we only win when there is a healthy, financially beneficial, and clean ecosystem
3) Reduce costs for good and risk-reducing behavior:
    a. Offer transactional discounts when vendors use our compliance partners
    b. Limit monitoring revenues to LTV60 to give discounts to vendors who can monetize beyond the first sixty days

In order to drive wide acceptance, AppEsteem will employ a freemium model. Our services will be available for free, with premium features available.

Software Monetizers (apps, installers, download sites, advertising syndicates)

Validation and Certification

1) Free: Company registration

2) Paid: App certification allows the use of AppEsteem's seal. Note that small carrier apps may be "sponsored" by their bundler or download site

Self-Regulating Client Library (SRCL)

1) Free: Most features of SRCL will be available to be used at no cost. Software vendors can use SRCL to implement distribution policies and validate certification signatures, as well as get notifications of apps that forcefully "block" or "clobber" them
2) Paid: Sealed apps can take advantage of the client library's ability to enforce distribution constraints and entitlements

Analysis services

1) Free: Aggregated data reporting on app installs, invalid blocking of apps
2) Premium: Deeper analysis including blocking/distribution, time to live, application combinations, fraud analysis
3) Premium: Sealed apps from validated companies can use our enforcement team to help stop fraudulent competitors

Security Partners (antimalware vendors, platforms)

Web services

1) Free: Validation of seals and most up to date information regarding the apps. Access to approved validation and certification disclosures. Dispute handling and verification
2) Premium: App reputation insights, FN/FP alerts (on sealed apps), protection effectiveness insights

Alternatives to, and threats against, our approach

We welcome solutions that stop bad apps from reaching consumers. We will strive to partner with and assist any security partner who can help achieve our vision.

Some adware and antimalware detection tools have established whitelisting services for consumers to rely on. For instance, Qihoo 360, Tencent and Baidu in China have flourishing whitelisting operations for both Windows and Android apps. These whitelisting services require software vendors to apply to each service individually. AppEsteem will not directly compete with these services, but turn them into our security partners: if they trust our seals, we'll help make them more effective by letting them focus more on non-compliant applications and bundlers. We'll also alert them to practices and details of fraudulent players who are hurting the business of sealed apps.

Consumers can also use true white-list products to limit what is installed. Platforms could restrict any applications to just their stores. These products and stores could require their own certification and monitoring solutions, which would compete with us. AppEsteem plans to discourage this fragmented approach by offering them a better deal: in return for stores and white-list products becoming our security partners and trusting our seal, we will provide them free data, and we'll handle their dispute resolution. If the service and store become popular with consumers, AppEsteem will certify apps to their guidelines as well.

Because we've been open about (and even publish online) our business strategy and processes, another entity could decide this is a great space to enter. The Clean Software Alliance may decide to start their own enforcement arm, or license enforcement rights to multiple providers, setting up direct competitors to AppEsteem. This gives us the sense of urgency to be the first movers, to have a full supply-chain solution, and to establish our own independent relationships with both the security partners and the software monetizers.

There is a threat of the larger platforms implementing their own programs to solve this problem. For instance, the platforms could deliver a robust software monetization platform to vendors that solves enforcement and monitoring, yet restricts AppEsteem from participating. AppEsteem's best approach in this model is to show the platforms that partnering with or even acquiring AppEsteem is a better, less risky, more regulator-friendly approach than rolling out exclusive solutions.

What gets built

AppEsteem is delivering the systems to handle the above scenarios. There are client components, automation tools, analysis services, and web services.

Client software (runs embedded in the apps)

1) SRCL: The monitoring and enforcement library that can be compiled into various apps. The library will instrument the app and monitor behavior as well as fraud and blocking activities. The library will also self-enforce distribution policies for the carrier app, bundler, and software offers, and validate the embedded seal.
    a. 2016: Windows executables (C++ lib with auto-injected DLL for monitoring child processes)
    b. 2016: Chrome extensions (JavaScript module using aspect-oriented programming)
    c. 2017: Android APKs
2) IEEE Taggant integration work
3) Front-end workflow app (web) for vendors/compliance partners to monitor what's happening

Web services (web interfaces for handling vendor/partner interactions with us)

1) Company registration and partner sign-up/approval
2) Validation and Certification Interviews
3) Customer self-management of profile, authorized users
4) Payment handling systems for validations and certifications
5) Software vendor disputes, questions, and responses
6) App Intelligence/telemetry display

Automation software for handling internal workflow

1) Analysis tools for lab validation of the software's use of SRCL and the seal
2) Signing services for applying AppEsteem seals and distribution constraints
3) Workflow tools to track, pipeline automation for getting the work done

Big Data analysis services (insights from telemetry)

1) Compliance monitoring
2) Distribution constraints monitoring
3) Fraud analysis
4) Invalid blocking analysis

Our Partnerships

Partnerships help us drive customers our way, defend our solutions from competition by being more complete and valuable, add data to our app intelligence, help us scale where we can't handle the load, and complete our story of certifying and monitoring the entire software monetization supply chain.

Relationship	What we provide them	What we expect from them	The Money
Security Partners	• Disclosures from validated vendors and certified apps. • Anonymous/aggregated non-certified telemetry	• Trust our seal, use latest data • Don't let our data be used to compete against us • Give actionable reasons when blocking sealed apps	• Our service is free. Future: we could offer measures of their effectiveness as they fight against the bad guys.
Compliance Officers	• Advertising for new customers • Telemetry and disclosures/commentary for their clients' apps • Workflow for accepting clients and approving disclosures before submittal.	• Detailed review and approval of the disclosures • Regular review of customer telemetry • Feedback on proposed certification and validation criteria changes	• Free for compliance officers. We give discounts on validations and certifications if customers use compliance officers.
Investigators and Certifiers	• Copy of the disclosures (and related ones) • Data of their previous or same-owned submissions/results. • Behavior graphs we've assembled • Buy in bulk: JoeSecurity, Reputation	• Investigators: Insights into the company and its business practices, helping us determine risk. Periodic monitoring of company. • Certifiers: scorecard results, review during disputes, periodic AV scans and detection alerts	• Pay per investigation/certification
Integrated service providers	• Advertising for customers • Service configuration • Collect and process payment on behalf of service provider	Provide information for appropriate billing and summarized results Provide the services at the lowest offered price point: • URL/File Monitors: Landing site URL and file download/inline install blocking • Traffic Analyzers/Curators: Landing page monitors and blockers to ensure that non-fraudulent traffic is not rewarded • 3rd Party Reviewers: validate/vouch for app value statements. • Payment Processors: handle in-app purchases	• We charge 10% commission, as well as rights to the inputs/outputs of the data flowing through configuration and summarized results.
Recommended service providers	• Encourage our customers to use these services	Provide aggregated and reputational data Provide the services at the lowest offered price point: • Payment processors: handling payment, returns Ad Syndicators: providing trusted feeds for in-app and in-browser ad injection	• We receive 1% commission on revenues, forwarded to us by the trusted service providers, along with rights to the aggregated and reputational data.
Enforcers	• Hints and maybe pass-through evidence of fraudulent behavior	Public relations	• No charge

Our Team

During its first four months of operation, AppEsteem has hired, contracted, or planned for the following staff:

1) Engineering (current: 8 + 3 TBH)
    a. Product manager
    b. Development team
        i. Two service-side engineers for workflow, telemetry handling, storage
        ii. Four client-side engineers for Windows, Chrome, and Android
        iii. One user experience engineer
        iv. Automation engineer to build analyst workflow components
        v. Two big data analysts for fraud detection and data visualization
2) Operations (5)
    a. COO, to attract, sell, operationalize, and support our customers
    b. General Counsel to manage legal issues, drive security partnerships
    c. Business Development to drive revenue-based ecosystem of partnerships
    d. Validation Manager writing validation policies and managing investigations
    e. Certification Manager driving criteria and managing approvals
3) Advisors to fill our gaps (4 + 2 TBH)
    a. Marketing Advisor for appropriate sales and marketing discipline and maximizing opportunity
    b. Industry Advisor to understand the monetization industry and trends plus predict future reactions
    c. Services Architect Advisor to oversee backend development
    d. Client Architect Advisor to drive client code quality and performance
    e. Forensics Investigator to help gather evidence of fraudulent behavior
    f. Security Advisor to drive proper implementation of seals

Beyond these employees and contractors, we plan to use business and data partnerships to scale out the work required for the company validations and app certifications:

1) We are identifying service providers for reputation of companies, domain names, apps, and URLs. We have a list of candidates, and we're currently vetting and selecting them.
2) For app certification, we have licensed Joe Security's analysis services. We are negotiating with an antimalware vendor to do the app certifications as piecework. We plan to use IEEE's Taggants as the basis of our seals, and will be contracting with them to become a provider.

Critical success factors

To be successful, AppEsteem needs to successfully deliver the following:

1) A set of guidelines acceptable and desirable by both security partners and software monetizers
2) The majority of platform and antimalware vendors trusting our seal
3) Recruit enough business providers and partners to complete an efficient ecosystem
4) Generate enough revenue to cover our costs of providing our service
5) Deliver appropriate technology that is performant
6) Run a successful pilot program
7) Priced aggressively enough to encourage partnership over competition
8) Fast enough to encourage regulators and platforms to give self-regulation a chance