VERACODE | FACT SHEET

BENEFITS

- ✓ Easily upload and test all mobile apps — whether built in-house, outsourced or downloaded from app stores.
- ✓ Identify risky behaviors and vulnerabilities inherited from third-party components and libraries.
- ✓ Address major platforms including iOS and Android.
- ✓ Detect risky mobile apps that need to be secured with app wrapping or container technologies.
- ✓ Catch risky mobile apps before offering them to enterprise app stores.
- ✓ Integrate security intelligence with widely-used MDM systems via APIs.
- ✓ Enforce enterprise policies with fine-grained controls.
- ✓ Help enterprise developers remediate mobile vulnerabilities early in the SDLC

Mobile Application Security

Reduce mobile application risk — while balancing innovation & control

Veracode's cloud-based solution helps mobile teams achieve the correct balance between innovation and control. We help effectively manage the security risk posed by the mobile apps that your organization builds, buys or downloads. Our solution provides the intelligence to protect against attacks and verify compliance with corporate risk and privacy policies.

Veracode's mobile application security solution combines automated code assessments with expert remediation services that enable IT teams to rapidly secure mobile applications in agile development environments — without slowing innovation.

Behavioral analysis inspects all application actions in real-time, in a controlled sandbox, to expose risky and malicious behaviors such as exfiltration of sensitive data to unknown entities. To determine a risk rating, these results are then compared against millions of known applications, both malicious and safe, in Veracode's reputation knowledge base.

The application is also assessed using binary static analysis to identify hidden malicious capabilities and common coding vulnerabilities such as buffer overflows and information leakage. Plus it integrates seamlessly with agile development processes and tools including IDEs such as Eclipse and Visual Studio; build servers like Jenkins and Team Foundation Server (TFS); and issue tracking systems like JIRA and Bugzilla.

Our comprehensive policy engine provides administrators with the ability to create fine-grained controls to manage mobile apps that violate enterprise policies, enabling the productivity benefits of BYOD (Bring-Your-Own Device) without sacrificing security in the process. To mitigate enterprise risk, our mobile security intelligence integrates with leading mobility device management (MDM) solutions to actively enforce policies on end-user devices. Veracode has established partnerships with MDM vendors including IBM/Fiberlink, Good Technology, MobileIron, and VMware/AirWatch.

Automated Cloud-Based Assessments

Behavioral Analysis

Behavioral Analysis is a security assessment methodology for mobile apps that provides insight into the risks posed by mobile app behaviors. It compliments traditional static and dynamic assessment methodologies which find security flaws and weaknesses in the application's code. Behavioral Analysis is designed to inspect mobile applications during operation for risky or malicious behaviors—such as exfiltrating and transmitting sensitive data to unknown entities. An app's risk rating is quantified in comparison to millions of data points from public applications. Behavioral analysis comprises:

Static Code Inspection: The executable code is inspected statically to identify risky capabilities such as access to sensitive data, contact lists, location, browser history, system logs and SIM card identity information; monitoring and recording of phone calls;

HIGHLIGHTS

Veracode secures all of your mobile apps, covering the three primary deployment methods:

- ✔ Mobile apps that you build. Automated assessments enable rapid innovation without sacrificing security.
- ✔ Mobile apps that you buy. Comprehensive behavioral analysis identifies violations of enterprise security and privacy policies.
- ✔ Mobile apps that users download. Security intelligence mitigates mobile risk as part of your corporate BYOD program.

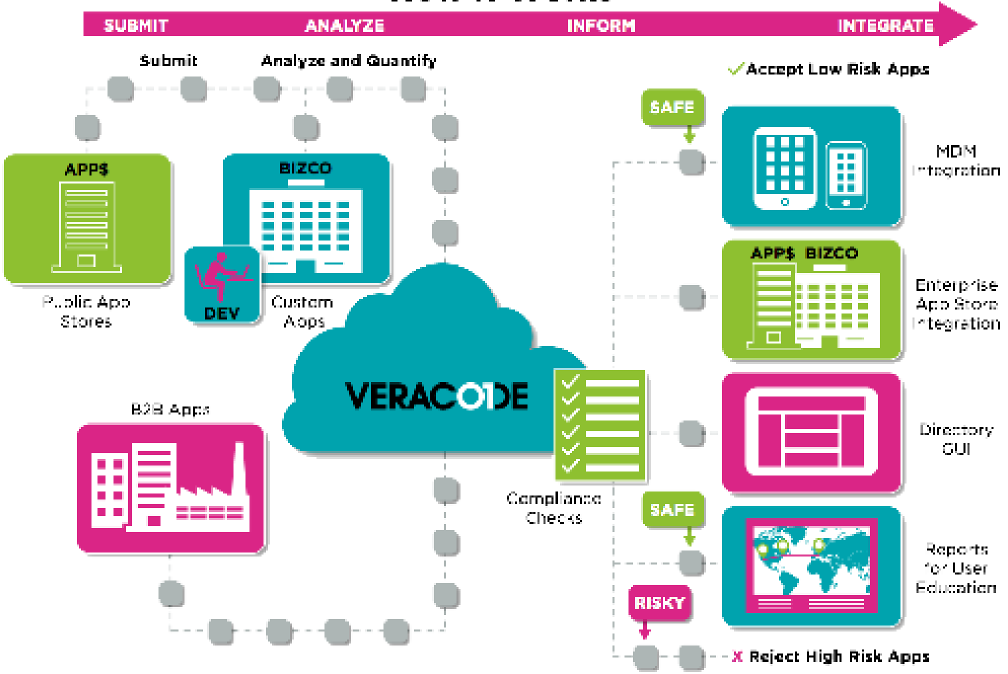
and device permissions that are native to the operating system API or custom-defined by developers. For example, Veracode research has revealed 67 percent of top mobile apps can access, add or edit address book contacts.

Dynamic Behavioral Analysis: The application is executed in a sandbox and instrumented to produce behavioral information such as GeoIP maps identifying data exfiltration; inbound and outbound IP addresses and domains; the data sent and received by the app during operation; and the files created, changed or deleted by the app during operation. Our research has shown that the top mobile apps send data to unknown entities located throughout the world.

Actionable Malware Rating: The malware rating indicates how likely it is that the app is malware, in other words the more your app behaves like malware, the worse the malware rating will be. We quantify this rating by analyzing the application's code capabilities and real-time behavior, comparing it against millions of data points from mobile applications, both malicious and safe. This generates a malware rating from 0 to 10. An application with a rating of 9 or 10 is classified as malicious and should be prevented by corporate policies from being installed.

Policy Engine: Every enterprise is different in the level of risk they are willing to take on—and the types of application behaviors they consider risky. Our comprehensive policy engine provides administrators with the ability to create custom policies, based upon fine-grained attributes, enabling the productivity benefits of BYOD without sacrificing security in the process.

How It Works



1. SUBMIT: Applications are auto-submitted using APIs or interactively via a simple web interface to our cloud-based platform.

2. ANALYZE: Dozens of analyses are performed, both statically, to identify how the application works and dynamically as the application runs in a sandbox, to identify hundreds of code vulnerabilities and risky app behaviors.

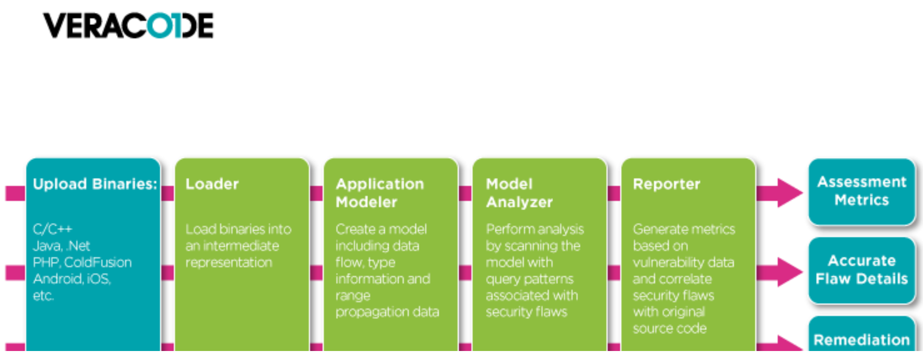
3. QUANTIFY: Advanced machine learning technology generates a risk rating for each application by comparing its behavioral profile to millions of data points from known applications, both malicious and safe.

4. INFORM: Our static and behavioral intelligence informs your policy development process, an important step for mobile application security programs. Our policy engine provides administrators with the ability to design and test rules before they are deployed for business units, geographies or workgroups.

5. ENFORCE: Integrate intelligence from our cloud-based platform with leading MDM solutions such as IBM/Fiberlink, MobileIron and VMware/AirWatch, or with custom in-house solutions via APIs, to enforce policies on end-user devices and enterprise app stores.

Binary Static Analysis (SAST)

Static Application Security Testing (SAST), or "white-box" testing, finds common vulnerabilities by performing a deep analysis of your applications without actually executing them. Unique in the industry, our patented binary SAST technology analyzes all code — including third-party components and libraries — without requiring access to source code.


VERACODE
Upload Binaries:
C/C++
Java, .Net
PHP, ColdFusion
Android, iOS,
etc.
Loader
Load binaries into an intermediate representation
Application Modeler
Create a model including data flow, type information and range propagation data
Model Analyzer
Perform analysis by scanning the model with query patterns associated with security flaws
Reporter
Generate metrics based on vulnerability data and correlate security flaws with original source code
Assessment Metrics
Accurate Flaw Details
Remediation

Mobile apps can be auto-submitted from developer build servers for binary SAST assessment. SAST analyzes binary code to create a detailed model of the app's data and control paths and find critical vulnerabilities such as buffer overflows.

SAST supplements threat modeling and code reviews performed by developers, finding coding errors and omissions more quickly and at lower cost via automation. It's typically run in the early phases of the Software Development Lifecycle because it's easier and less expensive to fix problems before going into production deployment.

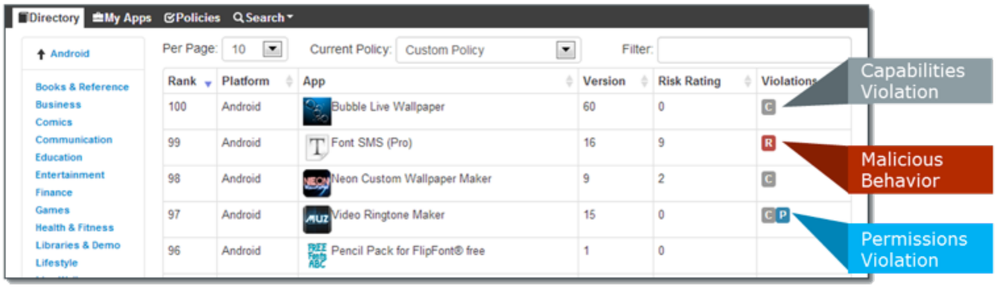
SAST identifies critical vulnerabilities such as buffer overflows, unhandled error conditions and potential back-doors. Our binary SAST technology delivers actionable information that prioritizes flaws according to severity and provides detailed remediation information to help developers address them quickly.

Reputation Service

Veracode's App Reputation Service provides behavioral intelligence about mobile applications to help you determine which mobile apps violate enterprise policies for security and privacy. Our integration with mobile device management (MDM) solutions helps you act on those policy violations to enforce compliance.

Intelligence Directory: We provide detailed intelligence about the most frequently downloaded Android and iOS applications, including indicators related to exposing corporate intellectual property, data leakage of personally identifiable information

(PII), transmitting data to suspicious geo-locations, and advanced persistent malware. This directory intelligence empowers enterprises to tightly manage “Bring Your-Own-App” risks while enabling employee productivity through the implementation of granular policies.



Per Page: 10 Current Policy: Custom Policy Filter:

Rank	Platform	App	Version	Risk Rating	Violations
100	Android	Bubble Live Wallpaper	60	0	C
99	Android	Font SMS (Pro)	16	9	R
98	Android	Neon Custom Wallpaper Maker	9	2	C
97	Android	Video Ringtone Maker	15	0	C P
96	Android	Pencil Pack for FlipFont® free	1	0	

Enforcement: Veracode enables security teams to develop granular policies to identify and manage risk and privacy violations in all of your apps, including predefined policies for:

- Data Loss Prevention — writing to external storage or social streaming
- Suspicious Security Behavior — rebooting the phone, recording phone calls or automatically sending emails
- GeoLocation Privacy — monitoring device location
- Personal Privacy — accessing contact lists, location or browser histories

MDM administrators can quickly determine which applications are allowed (whitelisted) or prohibited (blacklisted). You can then associate these apps with rules to specify the consequences of being out of policy, such as:

- Selective removal of apps or data from the device
- Prevent access to back-office business services and data

To learn more, see: www.veracode.com/products

Veracode’s cloud-based service and programmatic approach deliver a simpler and more scalable solution for reducing global application-layer risk across web, mobile and third-party applications. Recognized as a Gartner Magic Quadrant Leader since 2010, Veracode secures hundreds of the world’s largest global enterprises, including 3 of the top 4 banks in the Fortune 100 and 25+ of the world’s top 100 brands.

VERACODE
The Most Powerful Application Security Platform on the Planet