VERACODE | FACT SHEET

KEY FEATURES

- ✔ The inventory of apps installed across all of your company's managed devices is automatically submitted to Veracode's cloud-based service for behavioral analysis.
- ✔ Veracode identifies apps that have high malware risk ratings or are out of compliance with your app privacy policies (e.g., geo-location tracking) or security policies (e.g., cryptographic issues).
- ✔ Veracode's app reputation service automatically populates IBM Fiberlink's MaaS360 portal, enabling you to enforce actions when a risky or non-compliant app is identified.
- ✔ Compliance reporting is centralized via the MaaS360 portal.

Mobile App Reputation and Risk Management for IBM Fiberlink

Manage Mobile App Risk with Granular Policies

Veracode's cloud-based app reputation service provides behavioral intelligence about mobile apps to help you determine which apps violate corporate policies for security and privacy. Our integration with IBM Fiberlink MaaS360 uses automated workflows and centralized policies to give IT full visibility and control of app risks in a scalable way.

Secure enterprise mobility is no longer just about controlling email and managing device settings. Today, mobile apps are unleashing the true potential of mobile devices. The enterprise mobile app universe is expanding rapidly to include:

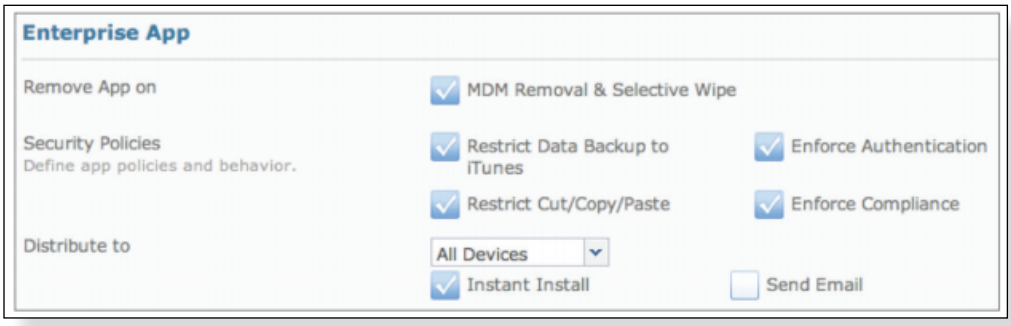
- Apps downloaded by employees from app stores, under BYOD programs
- Business apps that access back-office resources
- Apps made available from enterprise app stores

The challenge is finding the balance between enabling employee productivity and efficiently reducing enterprise risk. Enterprises need the power to distribute, manage and secure mobile apps critical to their business on both personal and corporate-owned devices.

Enforce App Security Policies Across All Devices

Integration between MaaS360 and Veracode enables IT teams to automatically enforce what actions to take when Veracode identifies apps that are not compliant with policy or have a high malware rating. Using MaaS360, administrators can:

- Blacklist, whitelist & assign required apps
- Receive real-time alerts of compliance violations
- View graphical reports of security & compliance history



IBM Fiberlink MaaS360 Policy Enforcement Options

VERACODE

FACT SHEET

KEY BENEFITS

- ✓ **Unprecedented visibility and control of app risks through deep integration of Veracode's mobile application reputation service with IBM MaaS360 Enterprise Mobility Management**
- ✓ **Single portal for complete app risk visibility, policies, compliance and reporting**
- ✓ **Proactive review of application risks and malware ratings before a public app is deployed**
- ✓ **Analysis of private enterprise apps to prevent data leaks, built right into mobile application management workflows**
- ✓ **Security policies and an automated compliance engine take immediate action once risky apps are identified**

• Limit native apps on a device (e.g., YouTube)

MaaS360 administrators can also configure automated enforcement actions based on risky apps identified by Veracode, such as:

• Notifying device users of non compliance

• Restrict network resources (e.g., no VPN)

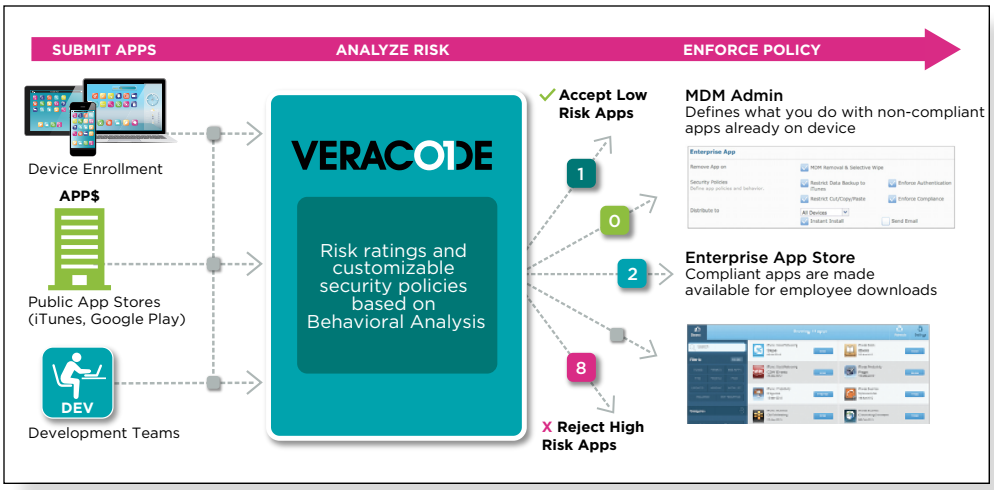
• Block access to corporate email

• Performing a remote wipe of selected apps

How Veracode App Reputation Works

Transparent to the user, apps are automatically submitted to Veracode's cloud-based app reputation service, which performs dozens of automated static and dynamic behavioral analyses on each app. These analyses identify what the code is capable of doing (code inspection), what the app actually does when run in a sandbox (dynamic behavioral analysis) and checks the app for known malware as identified by the top 50 antivirus research firms. Veracode's cloud-based service then utilizes an advanced machine learning algorithm to compare the behavior of the app to a vast database of known malware. The more the app behaves like malware, the worse the malware rating will be.

Additionally, security teams can create customized app security policies via the Veracode dashboard. Policies can include malware ratings, code inspection capabilities, and Android permissions, such as writing to external storage, allowing security teams to precisely specify which mobile apps violate enterprise policies for security and privacy.



To learn more, please visit: http://www.veracode.com/products/mobile-application-security

Veracode's cloud-based service and programmatic, policy-based 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