appgate

MOBILE APPLICATION PROTECTION

Malware and fraud attacks have moved from desktop browsers to the mobile apps, where end users now spend most of their time online.

Cybercriminals are leveraging security vulnerabilities and social engineering to infect mobile devices and steal the sensitive data that enables account takeovers. Secure applications with mobile-centric risk assessment and the detection of malware behavior, such as app spoofing and pharming attacks.

Targeted Attack Protection

Pharming

Identify and repair host file edits.

Man-in-the-Middle Attacks

Identify app certificate fraud to disable Man-in-the-Middle attacks.

Overlay Attacks (App Spoofing) (Only for Android)

Detect overlaying in banking applications to protect against attackers harvesting the personal information and login credentials of your end users.

Repackaged Apps (Only for Android)

Identify if the bank application has been modified.

Smishing Protection (Only for Android)

Uncover harmful Smishing attacks found within the SMS text messages on your end users' smartphones, so you can blacklist known and emerging threats.

Risk-Based Authentication

Device Risk Assessment

Use Detect Safe Browsing Mobile's Risk Controller interface to restrict access and functionality based on factors such as whether a phone is jailbroken, rooted, infected, face down, connected to public Wi-Fi and much more.

Secure Storage

Encrypts and protects data at rest in the application to prevent unauthorized access to the sensitive information it may contain.

BENEFITS

Eliminate the risk of credential compromiseon mobile

Protect your customers from application overlay, phishing, pharming and Man-in-the Middle attacks

Ensure that your app is running in a safe environment with a risk-based access policy through our Risk Controller™

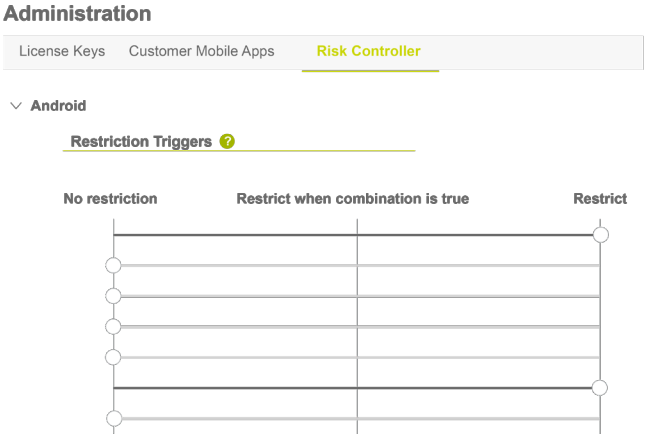
Risk Controller: Part of the Detect Safe Browsing Mobile Solution

Set your risk tolerance and see metrics related to threats detected on your platform with DSB Mobile's Risk Controller feature.

Risk Controller at a Glance

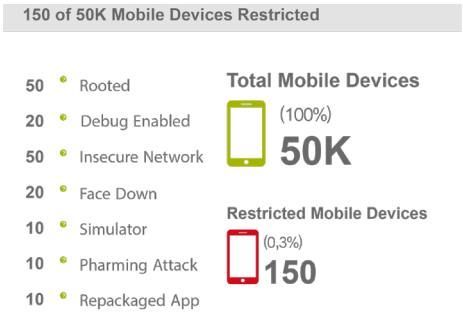
Take Control of Risk

Restrict, partially restrict or allow devices detected with each risk factor according to your own tolerance level.



Visibility into Risk Rules

See metrics on how many devices gain access or are restricted when trying to connect to your platform.



RISK CONTROLLER BENEFITS

- Instantly set your own risk parameters
- Discard inflexible one-size-fits-all mobile risk tolerance
- No more 'black-box' risk settings; Risk Controller is transparent and easy to use
- Adjust risk level settings at any time, without relying on a vendor or middleman to do it for you

CONFIGURABLE RISK FACTORS

- Jailbreak/Rooting
- Insecure Wi-Fi network connection (only for Android)
- Device placed face down
- Running application on a simulator
- Connected to another device in debug mode
- Modified host file in a pharming attack
- Running a repackaged App (only for Android)

About Appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Learn more at appgate.com

appgate