PROMON

Solution Brief

Malware Protect for Android

Promon offers defense-in-depth mobile malware protection

Defending against mobile malware has shifted from identifying the known bad and allowing the known good to detecting untrustworthy runtime conditions, and organizations need to take a layered security approach that meets regulations and maintains resilience.

What is mobile malware protection?

Attackers often employ a variety of techniques, including repackaging and social engineering, to trick users into downloading malware.

Malicious software and supporting attacker infrastructure has fingerprints, or indicators of compromise (IoCs), that can be detected by security controls.

For example:

- File names and hashes
- IP addresses and domain names
- URLs
- Behavioral indicators

While there are a variety of security controls that can be used to detect malware, a layered solution that employs scanning, threat intelligence, behavioral analysis, and runtime protection maximizes efficacy and resilience when defending mobile apps.

Why Malware Protect for Android?

Regulatory frameworks require the use of scanning as part of a broader defense-in-depth security posture to combat malware. For example, detecting specific malware within the banking sector, which often targets Android devices by tricking users into installing malicious apps.

Scanning for known malicious apps provides a deterministic and controlled approach for detecting malware, using curated intelligence as input to detect pervasive threats using predefined indicators of compromise.

Because zero-day malware has no known indicators of compromise, it is important to take a layered approach for defense, including enforcement of runtime integrity, since attackers often abuse platform features to manipulate app behavior.

What is included with Malware Protect for Android?

Malware Protect for Android includes a Malware Scan add-on to Shield for Mobile:

- Malware Scan enables detection of known malicious apps on an Android device.
- Shield for Mobile protects against unknown and zero-day threats through runtime integrity and behavioral defenses.

How is Malware Scan Implemented?

The following is needed to implement Malware Scan:

- A Java 17 runtime environment
- An Android app and access to the original source code
- The Shield download package that includes the Malware Scan SDK and MalwareScanEncryptor.jar executable
- A list of known malware applications to run scans against

Malicious apps are specified in an encrypted JSON file, denoted by package name and APK hash:

```JSON
{
  "malware_applications": [
    {
      "appPackageName": "com.example.malware1",
      "apkHashSHA256": "a0b11d7d14b510efb989cd85d2ee6d34454498dadbac4e78cd294a5ca
    },
    {
      "appPackageName": "com.other.malware2",
      "apkHashSHA256": "99a1d3deda2504f6c783a4b838b7db2436b5f145c8546bff58a3eb89f
    },
    // etc...
  ]
}
```

Customers define and maintain the JSON file and can leverage data provided by regulatory bodies and from external threat feeds.

Why is Shield for Mobile needed?

Negative security approaches such as scanning for known malware is deterministic. Positive security techniques such as comparing behavior to an established safe baseline can catch zero-day malware, but at a performance cost and risk of false positives. Threat intelligence can only be provided after a security researcher defines the IoCs to scan for, or artifacts are discovered through behavioral analysis.

To address zero-day and unknown threats, organizations should complement malware scanning with runtime protection to enforce environmental integrity and to correlate predictive indicators of malware based on behavior, techniques, and effects.

By focusing on malware techniques and effects, sophisticated, zero-day threats can be detected through runtime analysis of malware behavior using predictive indicators of attack to deter bad actors from observing user interactions, capturing sensitive data, and interfering with application behavior.

For example:

- Accessibility services enabled on rooted devices
- Applications running in virtualized environments such as emulators
- Use of keyloggers, screen mirrors, screen readers, and overlays
- Attempts to manipulate behavior at runtime using hooking frameworks
- Interception of SMS messages to steal 2FA codes
- Evasion like hiding icons, blocking uninstalls, masquerading as system updates

How Malware Protect for Android can help you

Malware Scan
Detect malicious apps using a curated list of known malware

Runtime Protection (RASP)
Neutralize malware detected at runtime

Anti-Tampering & Integrity Protection
Ensure defenses are not disabled or bypassed

Better Together

Promon Malware Protect for Android detects known malicious apps with Malware Scan and ensures runtime integrity by identifying malicious behavior at runtime with Shield for Mobile. This combined approach detects known malware and novel malware, leveraging both indicators of compromise and indicators of attack.
Additional information on Malware Scan is available within the Promon Portal: docs.promon.io/malware-scan/latest

For more information on runtime protection, check out Promon Shield for Mobile: promon.io/products/shield-mobile

Promon AS
Cort Adelers Gate 30
0251 Oslo
Norway

You develop.
We Protect.

PROMON

Learn more at promon.io