SandBlast Mobile

2.72

Release Notes
Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Check Point SandBlast Mobile 2.72

For more about this product, see the SandBlast Mobile Product Page
https://www.checkpoint.com/products/sandblast-mobile/

More Information


Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 May 2018</td>
<td>iOS minor version, detection of Enterprise/Developer certificate</td>
</tr>
<tr>
<td>1 April 2018</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
2.72 Updates

1. Top Threats - dashboard widget.
The new widget display real time counters of threats on the dashboard. Each counter is colored according to threat risk level (Red - High, Medium – Orange, Low- Yellow). The circled counters are clickable and will lead to more related threat info.

Top Threats Risk

- 3 High Threats (Rough API, Network)
- 7 Medium Threats (Hacking Tool)
- 2 Low Threats (Device Tracking Tool)
- 30 Non Official App Store App
- 9 Location Tracking

- Total apps scanned: 17688

2. Microsoft Intune sync iOS app list
Following Microsoft new API release SandBlast Mobile now support iOS device app list. In order to enable MS Intune app list API please update the MTD connector settings in MS Intune.

For more information on MS Microsoft integration click the link

3. BlackBerry UEM 12.7.2 sync iOS app list
Following BlackBerry new UEM release 12.7.2, SandBlast Mobile now support iOS device app list. For more information on BlackBerry UEM integration click the link
4. iOS Proxy detection

iOS Proxy detection is a new feature that provides dashboard admin visibility on iOS devices which are configured to work with proxy or global proxy.

To enable the feature go to dashboard Policy settings -> Device and select the risk level of a device which is configured with proxy settings.

To white list a proxy which is in used by the devices go to dashboard Policy settings -> Wi-Fi and add the IP address of the proxy

5. iOS Enterprise & Developer Detection

The new iOS version 2.72.3943 supports the detection of Enterprise & Developer certificate which were installed on the iOS device.

Enterprise & developer certificate should only be installed on devices in case the device is used for development or the organization have internal app for its employees.

The risk level for certificate detection is set in the device security policy under the ‘iOS Security Settings’ it is recommended to set these settings as Low risk for the first time in order to get visibility on the current state of the devices.

Certificates which were detected on the devices will be displayed in the iOS Profile tab and dashboard administrator can white list the developers / Enterprise certificates.

Once the legit certificates were white listed it is recommended to change the Policy to High so users will get security alerts on the devices and can remove the Certificate which violate the organization policy.
Mobile Client Supported Platforms

iOS: 8.x, 9.x, 10.x, 11.x
Android: 4.x, 5.x, 6.x, 7.x, 8.x.