© 2019 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page http://www.checkpoint.com/copyright.html for a list of our trademarks.

Refer to the Third Party copyright notices http://www.checkpoint.com/3rd_party_copyright.html for a list of relevant copyrights and third-party licenses.
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 3.6
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>11 September 2019</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Version 3.6 Updates

Zero-Phishing

With more and more phishing campaigns being occurring on a whim, it is extremely important that any MTD solution can protect against the unknown. We are happy to introduce a major enhancement for our Phishing prevention – Zero-Phishing prevention powered by Check Point ThreatCloud and enhanced by machine learning algorithms.

How it works

- Phishing pages try to imitate legitimate websites, leading the user to believe this is the real site and enter sensitive information, including the username and password.
- Zero-Phishing is designed to detect zero-day phishing sites, namely, phishing sites that have not yet been reported. As opposed to “traditional” anti-phishing methods, which are mostly based on page reputation, Zero-Phishing actively evaluates the authenticity of the site based on several indicators.
- The Zero-Phishing engines will allow the user to load any page, but once he tries to enter credentials of any kind, the engines start to run, collect the relevant indicators and send them for analysis to ThreatCloud.
- Once there is a verdict, the engine will either allow the user to fill out their credentials in the site, or block the typing of credentials with an explanation to the user. During the analysis the user can see the web form with the input fields blocked by a “Scanning…” message.

Zero-Phishing is designed to protect the user while maintaining a seamless browsing experience. The scanning takes 1-3 seconds. No private data or sensitive page content is sent to the Zero-Phishing service.

Enable Zero-Phishing prevention to protect device users from unknown phishing attacks:
Zero-Phishing prevention events:

<table>
<thead>
<tr>
<th>Time</th>
<th>Severity Level</th>
<th>Attack Vector</th>
<th>Threat Factors</th>
<th>Event</th>
<th>Event Details</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 02 2019, 11:03:45</td>
<td>Critical</td>
<td>Network Security</td>
<td>Zero-Phishing</td>
<td>Blocked</td>
<td>Url: <a href="https://ngcpl.jin/rent/index">https://ngcpl.jin/rent/index</a>...</td>
<td>Android</td>
</tr>
</tbody>
</table>

Scanning process on device, block page and information card of the event on the SandBlast Mobile Protect application:
Download Prevention

End-users download 3rd party apps and configurations very frequently. Configuration profiles can be downloaded for different reasons, e.g. to connect to WiFi network. Third party applications can be downloaded to avoid payment for the official one, or if the official local marketplace does not have the required app. Since both end-user and admin are often reluctant to control all malicious download use cases, this new capability provides assurance that these non-regulated downloads will not put their data at risk.

How it works

- Once enabled by the admin, downloads from 3rd party stores are prevented (does not affect the official app stores)
  - iOS - Includes both apps and configuration profiles.
  - Android - Includes apps.

Download prevention events:
HTTPS Inspection

Attackers constantly explore new attack techniques. To make detection harder, they often use protocols that encrypt traffic, usually widely supported HTTPS (HTTP over SSL/TLS).

We are proud to introduce you to the Check Point cutting edge technology of HTTPS inspection on mobile devices. HTTPS traffic from mobile browsers will be inspected for malicious payloads and resources without leaving the device itself, to provide the best grade of security without compromising user privacy. Risky and malicious content will be blocked, whether delivered by a plain or an encrypted protocol.

How it works

- Once enabled by the admin, the end user will install a Root CA on their device.
- Afterwards, any browsing in an internet browser (not apps) will be fully inspected locally through ONP.
Broken HTTPS blocking page:

This website may be impersonating expired.badssl.com to steal your personal or financial information. You should go back to the previous page.

If you understand the risks involved, you can proceed to expired.badssl.com (unsafe)

If this classification is incorrect click here to report wrong category.

For more information, please contact your Help Desk.
**Android 10 Support**

SandBlast Mobile Protect application version 3.6 is fully compatible and certified to run on Android 10 (Q).

Related changes:

- Follows Android 10 changes that prevent an application from reading device identifiers like Serial Number and IMEI. For customers with MDM integration, Android 10 users may need to perform manual registration (similar to iOS). We are working with MDM vendors to provide automatic registration.

**iOS 13 Support**

SandBlast Mobile Protect application version 3.6 is fully compatible with iOS 13.

**Report a Problem Enhancement**

Many customers have users who do not have the native email client configured or need to send logs through a partner

How it works:

- Emails address of Report a problem feature can be customized so device users will send reports about SandBlast Mobile application issues to corporate email (by contacting Check Point Support).

- Customers with no native email client configured on iOS devices will be able to share logs with Check Point.

**Supported Mobile Client Versions**

- **iOS**: SandBlast Mobile Protect 2.60* and higher
- **Android**: SandBlast Mobile Protect 2.60* and higher

(*) Devices running the outdated version will continue to be protected, but will not receive policy changes

**Supported Mobile Client Platforms**

- **iOS**: 10.x, 11.x, 12.x, 13.x
- **Android**: 5.x, 6.x, 7.x, 8.x, 9.x, 10.x