TDR Test Methodology

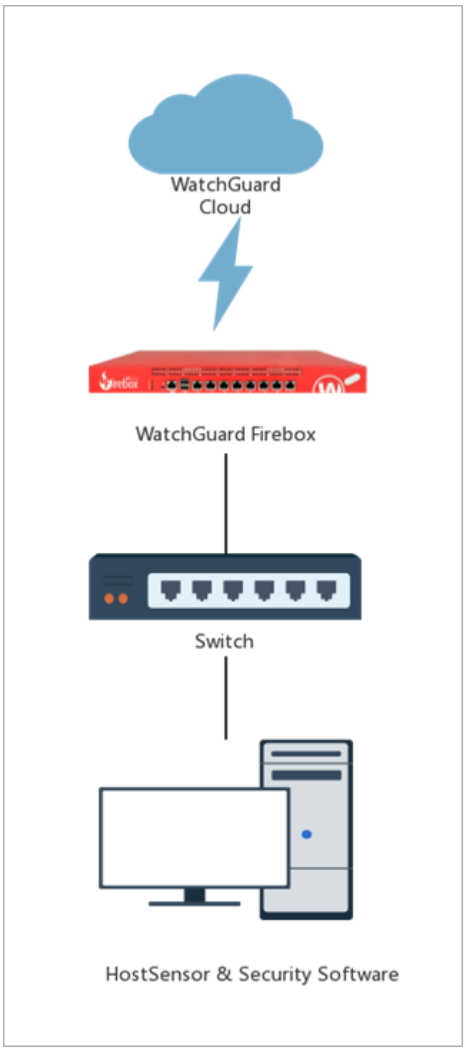
Test Methodology for Windows

TDR and Security Software

This document describes the test methodology to test integration of the Threat Detection and Response (TDR) Windows Host Sensor and third-party Security Software on the same host computer.

Test Topology

For these tests we installed both the TDR Host Sensor and the Security Software on the same host. All traffic from the host passes through a Firebox with TDR enabled.



Test Methodology

For this set of tests, we began with the default settings for both the Host Sensor and the Security Software.

1. Download and install the TDR Host Sensor while the Security Software real-time protection is running.

   Result – The TDR Host Sensor downloads and installs successfully, and runs without issues.

2. Download and install the Security Software while the TDR Host Sensor real-time protection is running.

   Result – The Security Software downloads and installs successfully and runs without issues.

3. Restart the Security Software while the TDR Host Sensor is running.

   Result – The Security Software restarts successfully.

4. Restart the TDR Host Sensor while the Security Software real-time protection is running.

   Result – The TDR Host Sensor restarts successfully.

5. Restart the host with both the TDR Host Sensor and Security Software real-time protection running.

   Result – Both the TDR Host Sensor and the Security Software start automatically and run without issues.

The TDR Host Sensor and Security Software can detect diverse types of malware at the same time. Detected threats could include files, registry values, and processes. To determine whether there would be a conflict when both applications detect malware, these tests were also completed.

1. Run Windows Update with the TDR Host Sensor and the Security Software real-time protection running.

   Result – Windows Update completes successfully.

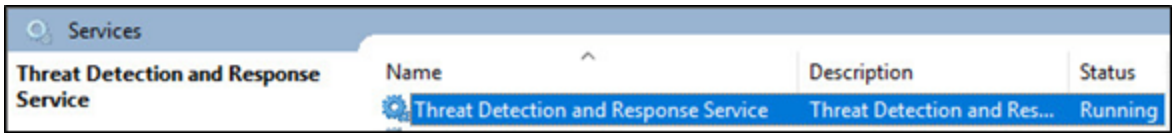
2. Uninstall the Security Software while the TDR Host Sensor is running.

   Result – The uninstall completes successfully.

3. Uninstall the TDR Host Sensor while the Security Software is running.

   Result – The uninstall completes successfully.

> ⓘ To stop and start the Host Sensor, in the Windows Services app, stop and restart the Threat Detection and Response Service.



About This Guide

Guide Type

Documented Integration – WatchGuard or a Technology Partner has provided documentation demonstrating integration.

Guide Details

WatchGuard provides integration instructions to help our customers configure WatchGuard products to work with products created by other organizations. If you need more information or technical support about how to configure a third-party product, see the documentation and support resources for that product.

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Guide revised: 1/18/2018

Copyright, Trademark, and Patent Information

Complete copyright, trademark, patent, and licensing information can be found in the Copyright and Licensing Guide, available online at http://www.watchguard.com/wgrd-help/documentation/overview.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter, @WatchGuard on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

Address

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

Support

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

Sales

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895