

# **Host Security**

## **Features in Different Editions**

### **Product Introduction**



## Copyright Notice

©2013-2018 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

## Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

## Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

# Features in Different Editions

Last updated : 2018-09-12 09:25:15

The main features available in different editions of Host Security are listed as follows:

Feature and Description	Basic Protection	Professional Protection
<b>WebShell Detection</b> Detects backdoor Trojan for common website scripts, including ASP, PHP, JSP, Python, and other scripting languages	√	√
<b>Hacker Tool Detection</b> Detects common hacker attack programs, such as DDoS Trojan, remote control and mining software	√	√
<b>Binary Virus Trojan Detection</b> Detects Trojan for binary executable viruses, including exe, dll, bin and other file types	√	√
<b>Password Cracking Attack Detection/Blocking</b> Issues alert for and intercepts common password cracking attacks by hackers	√	√
<b>Hacker Account Behavior Detection</b> Identifies suspicious hacker account information in the server	√	√
<b>Login Log Audit</b> Analyzes the login log in the server to identify malicious login behaviors	√	√
<b>Configuration Risk Item Detection</b> Checks configuration items of some system components to prevent vulnerabilities	-	√
<b>Weak Account Password Detection</b> Detects weak password information in the system account	-	√
<b>Web Component Vulnerability Detection</b> Detects Web vulnerabilities for Web components such as phpMyAdmin and WordPress	-	√
<b>Common Component Vulnerability Detection</b> Detects vulnerabilities for common component such as Apache, Nginx, Struts and Redis	-	√

Feature and Description	Basic Protection	Professional Protection
<b>System-Level Vulnerability Detection</b> Detects system-level vulnerabilities especially for operating system patches	-	√
<b>Vulnerability Repair Solution Push</b> Provides repair and protection solution for discovered vulnerability risks	-	√
<b>Zero-Day Vulnerability Intelligence Push</b> Pushes vulnerability intelligence at the earliest possible time based on Tencent's vulnerability intelligence	-	√
<b>Expert Service</b> Provides 5*8 security expert services online. You can request a callback by submitting a ticket.	-	√