Host Security

Product Overview

Product Introduction

©2013-2018 Tencent Cloud. All rights reserved.

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

Tencent Cloud

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.

Contents

©2013-2018 Tencent Cloud. All rights reserved.

Product Overview
Product Introduction

Last updated：2018-09-04 15:06:20

What is Host Security?

Host Security (HS) is a product that provides multi-dimensional security protection for CVMs based on the massive threat intelligence data and vulnerability information collected by Tencent over years. By leveraging machine learning, this product offers you a variety of security services such as hacker intrusion detection and vulnerability risk alert, allowing password cracking blocking, remote login alert, Trojan detection and removal, high-risk vulnerability detection and other security features. It can help your company deal with the major network security risks associated with servers and build a server security protection system to prevent data leakage.

Why do you need Host Security?

What security risks will your company face once your server is hacked?

- **Interrupted service**: Databases and files are tampered with or deleted, resulting in unavailability of service and corruption of system.
- **Data theft**: The act of hacker of stealing and selling company data compromises the customers' privacy and causes leakage of confidential data, leading to the damage to company's brand and churn of users.
- **Encryption by ransomware**: A hacker who intrudes into a company's server encrypts data and extorts money from the company by embedding irreversible encryption ransomware.
- **Unstable service**: A hacker runs mining and DDoS Trojan programs in a server to gain benefits and consume considerable system resources, causing the failure of server to provide services normally.

Host Security allows you to defense against the above problems and ensure the system and business security of your company website.

Key Features

Trojan Detection and Removal

©2013-2018 Tencent Cloud. All rights reserved.

Backdoor Trojan (also called Webshell) is a dynamic script (ASP, PHP, JSP, etc.) embedded in a website by a hacker who intrudes into the website by exploiting vulnerabilities. The hacker can bring the server under his/her control through Backdoor Trojan to upload/download files, execute commands and perform other malicious operations, posing a major threat to the website security.

With Tencent Cloud security platform's ability to collect malicious file samples across the network and Backdoor Trojan detection technology based on machine learning, Trojan Detection can accurately identify and remove all types of Trojan malicious files in real time while providing such features as malicious file detection and quick clean-up, thus removing the backdoor Trojan files at the earliest possible time to ensure user's server security.

Password Cracking Alert

When you can log in to your CVMs from the Internet, the CVMs is put at the risk of being intruded by illegal users through brute force attacks. Tencent Cloud Security is capable of monitoring if a CVM has come under brute force attack by multi-dimensional means. When any abnormality is detected, the system sends a notification to you via internal message or SMS.

Login Activity Audit

Based on your frequently used login location and malicious login source, the system analyzes the server's login log to identify the remote and abnormal login attempts and notifies you in real time. Through the analysis of server's account login activities, the system gives real-time alerts to you on the suspicious login attempts.

With CVM's log query feature, you can compare your login activities against the records in the logs to identify abnormal login attempts and take security measures.

Vulnerability Management

It issues real-time alerts and provides repair solution for high-risk vulnerability risks on the server, including system and Web vulnerabilities, helping your company deal with vulnerability risks quickly.

Asset Management

It manages servers by grouping and labeling them, giving you a quick picture of distribution of software, processes and ports in each server based on component identification technology.

©2013-2018 Tencent Cloud. All rights reserved.