

H3C SecCenter CSAP Advanced Threat Detection Engine

Product overview

Based on an in-depth understanding of advanced malicious threats and the long-term expertise of our team members, H3C launched the H3C SecCenter advanced threat detection (ATD) engine for the industry, which provides a set of security products and solutions for APT attack detection and defense.

The H3C ATD engine receives and detects malware through interfaces, and makes an in-depth analysis of the real intention of malware by using software virtual operation technology, sandbox anti-escape technology, and other technologies. It can detect advanced malicious threats such as APT attacks that cannot be detected by conventional means, and can conduct security collaboration with devices such as firewalls to block the further spread of threats and ensure network security for enterprises and organizations.

Features

Detection of mainstream applications and operating systems

Supports the detection of mainstream application software such as Word, Excel, PPT, PDF, HTML, JS, EXE, JPG, GIF, and PNG, and the detection of mainstream operating systems such as Windows XP and Windows 7.

Industry-leading detection performance

Provides industry-leading sandbox detection capability, with the number of sandboxes adjusted dynamically according to the detection pressure.

Anti-escape ability

Performs detection capabilities for VM detection or user interaction-based escape methods. In this way, it can effectively counter the escape behavior of malware.

Diverse ecological support

Provides standard interfaces, enabling third-party vendors to access files and return detection results.

Item	Function
Detection file format	Supports default file formats such as Office (Word, Excel, PPT, and RTF), WPS, PDF, HTML, JS, PE (EXE, DLL, etc.), swf, zipped packages, (ZIP, 7Z, RAR, etc.), script files (BAT, VBS, CMD, and PowerShell), and APK.
Dynamic sandbox detection	Supports the dynamic sandbox detection technology to detect known or unknown vulnerabilities and malicious codes such as Trojan horses, worms, viruses, and hacking tools. The type of sandboxes includes the system sandbox, document sandbox, and Web sandbox.
Network behavior simulation	Supports the simulation of various network protocols, such as DNS and HTTP.
Adaptive sandbox quantity	Supports automatic adjustment of the quantity of sandboxes according to the load of various

Item	Function
	sandboxes, to adapt to different network environments.

Ordering information

You can order the host and components of H3C ATD engine as needed.

Software Platform

Module	Description	Remarks
LIS-SecCenter CSAP-ATD-A	H3C SecCenter CSAP Advanced Threat Detection Product software license – advanced version	Required
LIS-SecCenter CSAP-ATD-E	H3C SecCenter CSAP-ATD-E Advanced Threat Detection Product software license – enhanced version	Required
LIS-SecCenter CSAP-ATD-P	H3C SecCenter CSAP-ATD-P Advanced Threat Detection Product software license – professional version	Required
LIS-SecCenter CSAP-ATD-A-1Y	H3C SecCenter CSAP-ATD-A 1-year signature database upgrade authorization letter	optional
LIS-SecCenter CSAP-ATD-E-1Y	H3C SecCenter CSAP-ATD-E 1-year signature database upgrade authorization letter	optional
LIS-SecCenter CSAP-ATD-P-1Y	H3C SecCenter CSAP-ATD-P 1-year signature database upgrade authorization letter	optional



New H3C Technologies Co., Limited

Beijing Headquarters

Address: Tower 1, LSH Center, 8 Guangshun South Street, Chaoyang District, Beijing P.R.China
Postcode: 100102

Hangzhou Headquarters

Address: 466 Changhe Road, Binjiang District, Hangzhou, Zhejiang Province 310052 P.R.China
Postcode: 310052
TEL: +86-571-86760000
Fax: +86-571-86760001

<https://www.h3c.com>

Copyright © 2023 New H3C Technologies Co., Ltd. All Rights Reserved.

Disclaimer: Though H3C strives to provide accurate information in this document, we cannot guarantee that details do not contain any technical error or printing error. Therefore, H3C cannot accept responsibility for any inaccuracy in this document.

H3C reserves the right for the modification of the contents herein without prior notification.