Huawei FireHunter-Cloud Sandbox

purchase and use at any time for defense against unknown threats

Overview

In recent years, data leakage incidents have become a regular occurrence. In 2016 alone, hundreds of millions of data records were leaked. Hackers often use constantly changing malicious programs of unknown origins to launch phishing, watering hole, and other types of attacks in order to steal critical data and cause damage to the IT infrastructures of enterprises. Attacks often exploit zero-day vulnerabilities and use advanced evasion techniques to bypass most currently available security measures, avoid multi-layer network protection and filtering, and create staging platforms for attacks within the internal networks of enterprises.

Huawei's FireHunter-Cloud sandbox solution creates cloud-based sandbox clusters, which are deployed in conjunction with Huawei's next-generation firewalls to provide a cloud detection service for advanced malicious software. Sandbox technology uses a simulated file execution environment to analyze and collect data on the static and dynamic behaviors of unknown software, perform behavior mode learning and comprehensive matching analysis in order to detect unknown malicious software, effectively prevent attacks from rapidly expanding in size, and prevent damage to core enterprise information systems.

Huawei's FireHunter-Cloud sandbox has an integrated access point at http://sec.huawei.com (SEC). In order to use the Portal, users must first register an account on the SEC website. All Huawei customers can register an account for free. After registering an account and logging in, the system will automatically choose whether to connect the user to the European or to the Chinese FireHunter-Cloud sandbox Portal depending on the user's geographical location. Users can use the Portal to manually upload files and view detection reports, and also bind their accounts to NGFW-type devices. After binding, users can view lists of files provided by devices and detailed detection reports of those files.

Key Features of the FireHunter-Cloud sandbox

Reputation system-based multilayer filtering of known threats:

The Huawei sandbox features a number of antivirus engines from leading antivirus solution vendors both in and outside China. After the FireHunter-Cloud sandbox receives a file, the sandbox will use all of its antivirus engines to scan the file for malicious content. The antivirus engines are highly effective, providing over 99% detection rates for known threats. With the detection by multiple antivirus engines, threats can be rapidly detected, and the threat data can be incorporated into the FireHunter-Cloud sandbox's final security report.

Static and dynamic analysis – finding unknown threats in minutes:

The FireHunter-Cloud sandbox's static heuristic detection technology is able to analyze binary code and shellcode in order to inspect file structures and file code for malicious content. Cloud dynamic inspection is predominantly based on antivirus virtual machine technology. It uses simulated IE, Adobe, and Windows software to create an antivirus virtual machine, after which malicious software is loaded into the simulated system. The virtual machine contains numerous behavior monitoring points that perform real-time monitoring of applications. When an application exhibits abnormal behavior, it is shut down and a virus report is submitted.

The FireHunter-Cloud sandbox's virtual execution environment technology is able to simulate Windows XP, Windows 7, and Windows 10 operating systems, and automatically select suitable virtual runtime environments. By monitoring API calling behaviors during the processing period, application files can be inspected to see if they are malicious in nature.

The FireHunter-Cloud sandbox's advanced anti-evasion technology uses interactive detection, file path inspection, virtual machine environment inspection, delay control, and environment inspection technologies to prevent malicious software from hiding from virtual machine inspections and to conduct rapid inspections of malicious files and provide inspection reports.

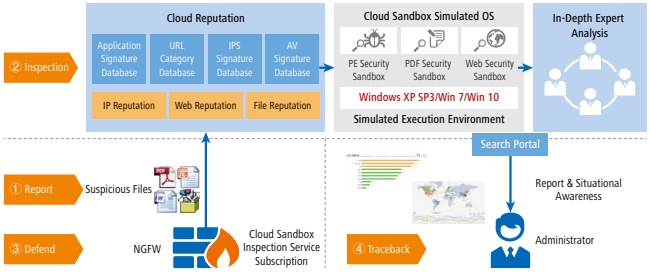

Figure 1 FireHunter-Cloud sandbox overall workflow

Detailed threat report:

Users can use their cloud accounts to log in to the portal and manually view inspection lists and inspection reports. Inspection reports show inspection results from multiple operating systems, detailed threat sandbox analysis, and recommended courses of action. Reports also contain information on the danger levels of detected threats, the nature of the threats, file information, shellcode content, packet capture when running the file, malicious file samples, file transfer traffic information, sample file behavior sequences, and single or batch downloaded compressed sample files.

A service that can be purchased and used at any time for easy and rapid deployment:

The FireHunter-Cloud sandbox can be used in conjunction with a local firewall that uses multiple restoration technologies, including fragment reassembly, anti-obfuscation, statistics-based identification, heuristic behavior identification, and SSL proxy decryption, to restore files within files and send the files to the FireHunter-Cloud sandbox for inspection. The FireHunter-Cloud sandbox license is easy to purchase and use so that the FireHunter-Cloud sandbox can be quickly deployed, catering to the needs of small- and medium-sized enterprises.

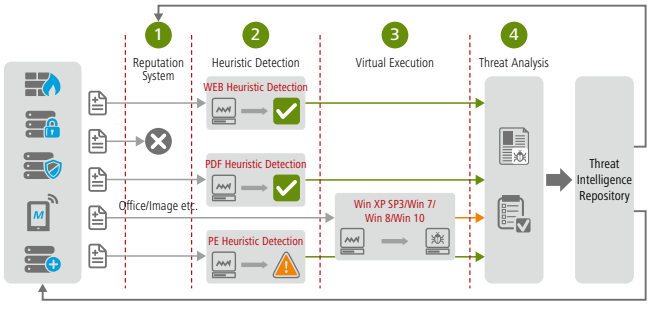

Figure 2 FireHunter-Cloud sandbox inspection model

Huawei FireHunter-Cloud Sandbox
purchase and use at any time for defense against unknown threats

Support from an expert team:

A team of security experts can analyze each malicious sample's activities and behaviors, compare them to a databank of millions of other samples and incorporate cloud-based threat intelligence to create a detailed picture of the sample's history, behavior and effect on a global scale.

Key Detection Capabilities of the FireHunter-Cloud sandbox

Huawei's FireHunter-Cloud sandbox is able to inspect many file types. Refer to the table below for more details. When a sample is uploaded manually, all of the file types mentioned below can be uploaded. When the local security device interworks with the FireHunter-Cloud sandbox, some file types will be restricted due to performance considerations. An example of this is when using the Huawei NGFW, only Windows executable files, MS Office 97-2003, MS Office, and PDF files can be uploaded.

Table 1 Virtual operating systems and major file types supported by the FireHunter-Cloud sandbox

Main Features	
Operating systems	Windows XP, Windows 7 32-bit and 64-bit, Windows 10 32-bit and 64-bit The FireHunter-Cloud sandbox selects the operating system to use for inspection depending on the file.
Portal-compatible internet browser	Supports Firefox version 46 and above, and Google Chrome version 50 and above.
Traffic restoration	Supports HTTP, SMTP, POP3, IMAP, and FTP protocol traffic restoration.
Script file types	Supports CMD, BAT, VBS, VBE, Ruby, PS1, ASP, PHP, and Python files.
PE file types	Supports compressed PE, EXE, and DLL files.
PDF file types	Supports PDF files (including compressed ones).
Web file types	Supports HTML/HTM, JavaScript, compressed web, Flash, and JavaApplet files; supports URL inspection.
Office file types	Supports Word, Excel, PowerPoint, RTF, and WPS files, and compressed Office files.
Image file types	Supports GIF, JPG, PNG, and TIFF files (including compressed ones).
Others	Supports SWF and COM files.

Benefits to Customers

1. **Detects unknown threats in minutes:** Real-time inspection of suspicious files and up-to-date reputation information synchronized in real time to networks, security devices, servers, and terminal devices.
2. **Improves a small enterprise's ability to defend against APT attacks:** FireHunter-Cloud sandboxes have stronger security inspection capabilities than local sandboxes and are able to conduct in-depth inspections of high-risk samples.
3. **Reduces sandbox deployment costs and period for small enterprises:** FireHunter-Cloud sandboxes are an alternative sandbox service for small- and medium-sized enterprises who cannot afford local sandboxes.

Service Subscription Information

FireHunter-Cloud sandbox customers can use the Portal to directly upload samples, or they can associate their local firewall with the FireHunter-Cloud sandbox via API ports to automatically upload samples. FireHunter-Cloud sandbox licenses support contract period of 1, 2, or 3 years.

Table 2 Firewalls that support FireHunter-Cloud sandbox services

Model	Description
The following apply to enterprise networks outside China.	
LIC-CS-1Y-USG63B	Cloud sandbox Inspection 1-Year Service (Applies to USG6320)
LIC-CS-3Y-USG63B	Cloud sandbox Inspection 3-Year Service (Applies to USG6320)
LIC-CS-1Y-USG63C	Cloud sandbox Inspection 1-Year Service (Applies to USG6330/50/60)
LIC-CS-3Y-USG63C	Cloud sandbox Inspection 3-Year Service (Applies to USG6330/50/60)
LIC-CS-1Y-USG63D	Cloud sandbox Inspection 1-Year Service (Applies to USG6370/80)
LIC-CS-3Y-USG63D	Cloud sandbox Inspection 3-Year Service (Applies to USG6370/80)
LIC-CS-1Y-USG63E	Cloud sandbox Inspection 1-Year Service (Applies to USG6390/6390E)
LIC-CS-3Y-USG63E	Cloud sandbox Inspection 3-Year Service (Applies to USG6390/6390E)
LIC-CS-1Y-USG66	Cloud sandbox Inspection 1-Year Service (Applies to USG6600)
LIC-CS-3Y-USG66	Cloud sandbox Inspection 3-Year Service (Applies to USG6600)
LIC-CS-1Y-USG9500	Cloud sandbox Inspection 1-Year Service (Applies to USG9500)
LIC-CS-3Y-USG9500	Cloud sandbox Inspection 3-Year Service (Applies to USG9500)
The following apply to carriers outside China.	
LIC-CS-1Y-E200E	Cloud sandbox Inspection 1-Year Service (Applies to E200E-N)
LIC-CS-3Y-E200E	Cloud sandbox Inspection 3-Year Service (Applies to E200E-N)
LIC-CS-1Y-E1KE	Cloud sandbox Inspection 1-Year Service (Applies to E1000E-N)
LIC-CS-3Y-E1KE	Cloud sandbox Inspection 3-Year Service (Applies to E1000E-N)

Model	Description
LIC-CS-1Y-E8KE	Cloud sandbox Inspection 1-Year Service (Applies to E8000E-X)
LIC-CS-3Y-E8KE	Cloud sandbox Inspection 3-Year Service (Applies to E8000E-X)
The following apply to enterprise networks and carriers outside China.	
LIC-CS-1Y-NGFWM	Cloud sandbox Inspection 1-Year Service (Applies to Switch NGFW Module)
LIC-CS-3Y-NGFWM	Cloud sandbox Inspection 3-Year Service (Applies to Switch NGFW Module)
LIC-CS12-NIP60	Cloud sandbox Inspection 1-Year Service (Applies to NIP6300&6610)
LIC-CS12-NIP60	NIP6300&6610 Cloud sandbox Inspection 2-Year Service (Applies to NIP6300&6610)
LIC-CS12-NIP66A	NIP6620 Cloud sandbox Inspection 1-Year Service (Applies to NIP6300&6610)
LIC-CS24-NIP66A	NIP6620 Cloud sandbox Inspection 2-Year Service (Applies to NIP6300&6610)
LIC-CS12-NIP66B	NIP6650&6680 Cloud sandbox Inspection 1-Year Service (Applies to NIP6300&6610)
LIC-CS24-NIP66B	NIP6650&6680 Cloud sandbox Inspection 2-Year Service (Applies to NIP6300&6610)