Huawei FireHunter 6000 series

Huawei FireHunter 6000 series sandbox product

Product Overview

Advanced Persistent Threats (APTs) often use social engineering to obtain contact information and send phishing emails to unsuspecting people. They exploit security vulnerabilities in Internet of Things (IoT) devices, and hide, without being detected, in high-value business assets to steal or compromise target information. Attacks are commonly seen in compromised infrastructure, such as the finance sector, resource suppliers, and government agencies, affecting people's livelihoods. Before launching attacks, perpetrators are usually well-prepared and wait patiently for their opportunity. Once attacks are launched, perpetrators usually use technologies, such as advanced evasion techniques in combination, to exploit known vulnerabilities. This makes the security devices that detect attack traffic ineffective.

Huawei FireHunter 6000 series sandbox products (hereinafter referred to as Huawei FireHunter) are a family of APT detection systems. They reassemble network traffic mirrored by switches or traditional security devices, and detect files transferred over networks in virtualized environments to detect unknown malicious files. Through credit scanning, real-time behavior analysis, big data-based correlation analysis, and cloud-end technologies, Huawei FireHunter collects and analyzes the static and dynamic behavior of target software programs to provide accurate detection results with the help of a unique behavior model library. Based on the results, Huawei FireHunter detects, blocks, and visualizes suspicious traffic streams, effectively preventing the spread of unknown threats and protecting business's core information assets. Huawei FireHunter is especially useful to finance and government agencies, resource providers, and high-tech enterprises.

Product Highlights

Multi-system simulation capabilities, ensuring comprehensive detection of unknown threats.

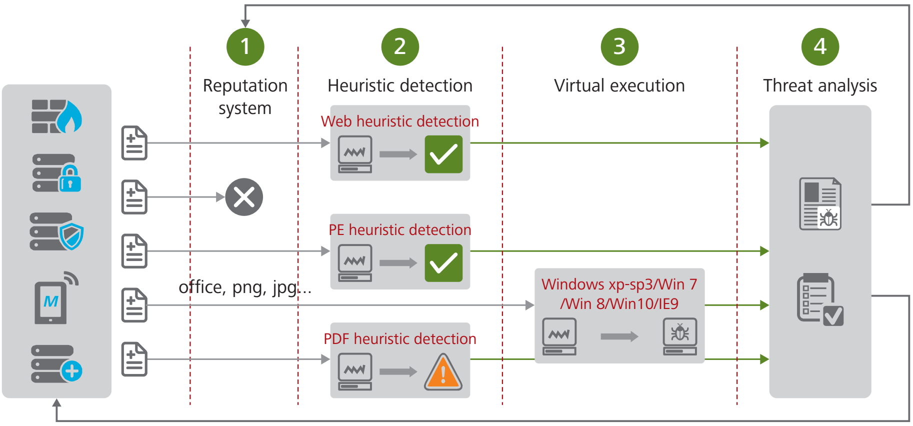
- **Comprehensive traffic detection capabilities:** Huawei FireHunter is capable of identifying mainstream file transfer protocols, such as HTTP, SMTP, POP3, IMAP, and FTP, and detecting malicious files transmitted using these protocols.
- **Detection of mainstream file types:** Huawei FireHunter is capable of detecting malicious codes contained in files, such as .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf, .html, .js, .exe, .jpg, .gif, .png, .swf, and .zip, created using mainstream applications.
- **Detection of web traffic:** Huawei FireHunter supports the detection of zero-day vulnerabilities on web pages, which makes Huawei one of just two vendors in the world to support such a detection function.
- **Simulation of mainstream operating systems and applications:** Huawei FireHunter is capable of simulating the behavior of Windows operating system, Internet Explorer, Microsoft Office suite, and Kingsoft WPS by default. This can be customized to suit your needs.

Multi-layer in-depth detections and rapid response in seconds, blocking unknown threats

- **Layered defense system:** Huawei FireHunter supports reputation matching, heuristic detection, and virtualized execution, ensuring Huawei FireHunter can tackle next-generation threats represented by APT attacks.
- **Industry-leading performance:** Huawei FireHunter provides industry-leading capability by analyzing 70,000 files per day. Multiple Huawei FireHunters can be deployed to form a cluster to expand performance.
- **Near-real-time processing capabilities:** Huawei FireHunter provides near-real-time processing capabilities, reducing the response time from weeks to seconds. In addition, Huawei FireHunter can work with the NGFW to provide online defense capabilities.

Multi-dimensional analysis, reducing false positives and improving the detection accuracy.

- **Multi-dimensional analysis capabilities:** Huawei FireHunter performs static analysis of code snippets, file format anomalies, and malicious script behavior to pin down suspicious traffic; performs dynamic analysis through instruction stream monitoring to identify malicious files and operations; performs correlated behavior analysis to determine whether traffic is legitimate.



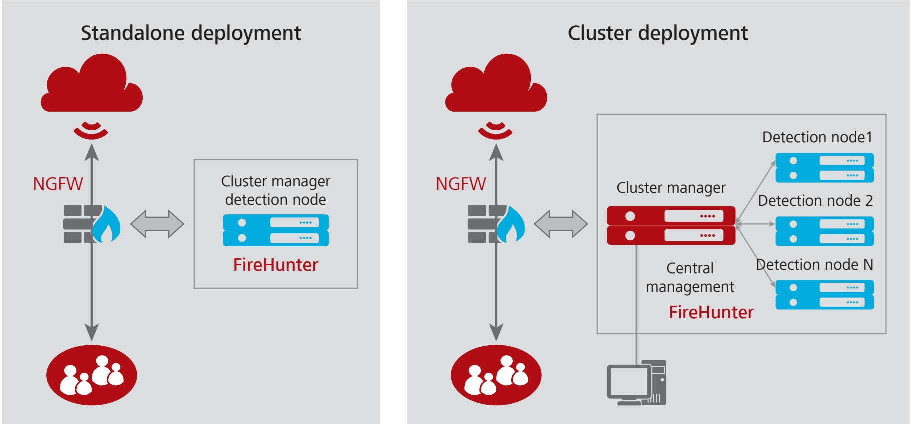
Product Deployment

Huawei FireHunter can be deployed in following modes:

Interworking with the NGFW, standalone deployment: The NGFW restores files and sends files to be detected to the sandbox.

Interworking with the NGFW, cluster deployment: The NGFW restores files and sends files to be detected to the sandbox cluster. Four FireHunter V100R001C20s or FireHunter V100R001C30s can be deployed in a cluster, In a cluster, a device serves as the management center, and other devices the detection nodes. The management center distributes files to detection nodes for load balancing and provides a unified detection result query interface.

Standalone deployment: Traffic is mirrored to the sandbox, which restores the traffic to files and detects them. Traffic can be mirrored using the mirroring port or optical splitter. In this scenario, the sandbox only detects files, and other security devices block files.



Specifications

Model	FireHunter 6000
Hardware configuration	• x86 server in a 2-U rack • Memory of no less than 128 GB • Two power modules for redundancy • Hard drive with a capacity of no less than 2 TB • SSD drive with a capacity of no less than 128 GB • 8 x GE electrical ports • 2 x 10GE optical ports