Hillstone Cloud-Sandbox:
Malicious File Identification and Detection Platform

Advanced Malware has become so sophisticated that it can easily evade traditional security solutions including firewalls, IPS and Anti-Virus technologies. To address advanced malware, the Hillstone Cloud Sandbox delivers a unique, advanced threat detection platform that can emulate the execution environment and analyze all activities related to malicious files, identify advanced threats and collaborate with existing solutions to provide rapid remediation.

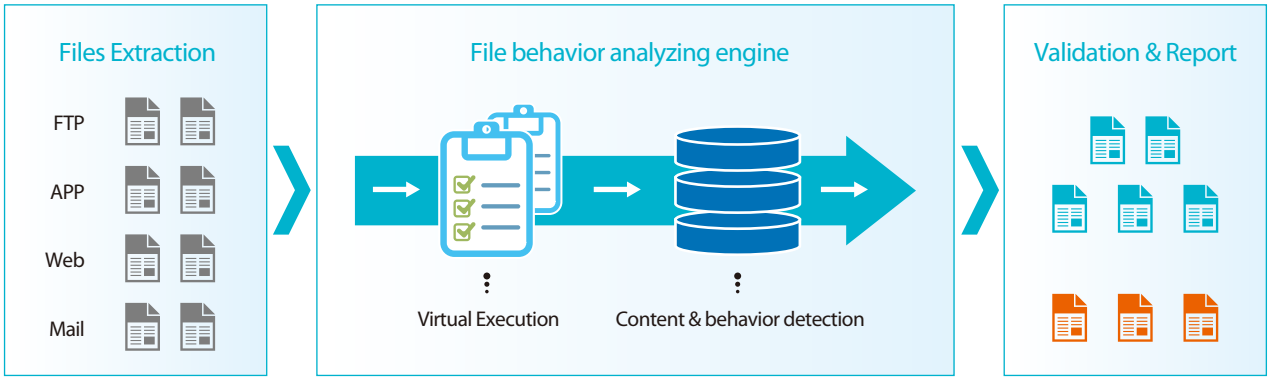
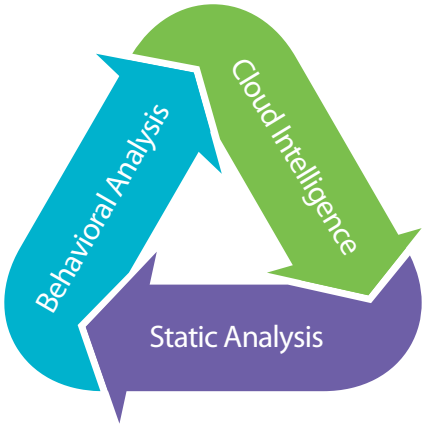


Figure 1. Hillstone Cloud-Sandbox

The Hillstone Cloud Sandbox is comprised of three modules: Static Analysis, Behavioral Analysis and Cloud Intelligence. The three modules work together to ensure the efficiency and efficacy of malicious files detection.



www.hillstonenet.com
Phone: 1-800-889-9860

Static analysis: Hillstone cloud sandbox executes static signature analysis of the files, such as identification of file types, file format, and the known malware signature. Additionally, the front filter technology (E.g. URL whitelist, file signature validation, sample database on cloud) can screen out the known threats to reduce the workload of sandbox.

Behavioral Analysis: Hillstone Cloud Sandbox can simulate multiple operation systems and running environments, and trigger file behaviors in the simulated environments that closely resemble real ones in production environments. The Sandbox uses a machine learning model to validate the file behavior.

Cloud Intelligence: By using threats intelligence information compiled globally from Hillstone network nodes, Hillstone Cloud Sandbox compares the static information and behavior of the files against the intelligence information, such as malware signatures, phishing websites and malicious domain names, and attaches every file with a risk evaluation score, rather than simply defining it as good or bad.

Through static analysis, behavioral analysis and cloud intelligence, Hillstone Cloud Sandbox detects malware with a low false-positive rate and high detection rate.

Product Highlights

High detection rate with both static and behavioral analysis

The malware sample database on the Hillstone cloud contains more than 1 billion samples. It quickly detects whether any uploaded file matches with the malware samples. Hillstone Cloud Sandbox can simulate running environments and trigger file behaviors such as creating processes, modifying registry and requesting back chain. Unknown threats can be detected by analyzing the file behavior.

Instant deployment of cloud infrastructure

Hillstone Cloud Sandbox is seamlessly integrated with existing Hillstone technology and solutions, such as the Next-Generation Firewall and Hillstone CloudEdge. It can be deployed instantly and seamlessly without network disruption.

Protection of encrypted traffic

Since SSL encryption technology has become popular, more and more applications use HTTPS. However, today's malware also uses SSL encryption technology to escape from detection. Hillstone Cloud Sandbox can decrypt the encrypted traffic and restore the files in the encrypted traffic. With this approach, malware can be detected, even if they are hidden in the encrypted traffic.

Measurements against the anti-sandbox technology

Hillstone Cloud Sandbox supports the identification and detection of anti-sandbox malwares. By hiding the sandbox processing information such as kernel model and registry information, Hillstone Cloud Sandbox can simulate the running environments. To avoid malware from escaping from detection, Hillstone Cloud Sandbox simulates manual and interactive operations and takes over the API, so that the malware behavior can be triggered.

Comprehensive threats information in the reports

Upon detecting malware and unknown threats, Hillstone Cloud Sandbox displays alarms and notifications, as well as comprehensive reports of malware behavior in the administration panel of the firewall. Network behavior, process behavior, file behavior, and file key information are displayed in the reports. The process for the attack is visualized through the Kill Chain analysis on firewall platforms, so that security administrators can take appropriate action.

Constantly updating signature database

Hillstone Cloud Sandbox generates threat intelligence based on the malware it detects and updates the intelligence information to the signature database of the Hillstone Next-Generation Firewalls. It helps administrators adjust security strategies to protect their IT resources from new newer and advanced attacks.

Specifications

Model	Files/Day	Recommended Platforms
Cloud-Sandbox 300	300	Hillstone E1000 Series, E2000 Series, E3000 Series, T1860, T2860, NIPS S600, S1060, S1560 and Hillstone CloudEdge
Cloud-Sandbox 500	500	Hillstone E5000 Series, T3860, T5860, NIPS S2160 and S2660
Cloud-Sandbox 1000	1,000	Hillstone E6000 Series

Version: EX-08.01-CloudSandbox-V2.0-0217-EN-01