

Splunk App for FireEye

Using Splunk to Combine Long-term Data Trending and Analytics with FireEye Data

FireEye

The FireEye™ Malware Protection System is the next generation of threat protection focused on combating advanced malware, zero-day and targeted APT attacks. FireEye's solutions supplement traditional security defenses, such as firewalls, IPS, AV and Web gateways.

FireEye provides dynamic analysis of zero-day attacks within a virtual environment. This yields real-time malware security intelligence that is then used to protect the local network. This intelligence can also be shared to all subscribers of the FireEye Malware Protection Cloud.

FireEye collects a variety of critical information such as the IP address, protocols and ports an attacker uses to communicate and distribute payloads. With this data, FireEye can block the activities of a compromised host. Even "patient zero" can be secured against sending out data or downloading more malware when FireEye systems are used inline. Detailed reports help system administrators identify infected hosts for clean up.

Zero-day, targeted malware enable advanced persistent threats to breach IT security, steal/alter/destroy sensitive data and exploit network resources. FireEye offers a new generation of network security threat protection that is being used by leading enterprises, government agencies and higher education institutions.

FireEye Web MPS Appliances integrate inbound and outbound protection in a turnkey system that deploys in minutes for rapid security ROI. They employ a sophisticated virtual execution engine to detect and block advanced known and unknown malware as well as block outbound malware transmissions. FireEye appliances allow you to:

- Actively analyze unknown code and suspicious Web objects
- Cut off outbound malware transmissions across multiple protocols
- Dynamically generate malware intelligence
- Block blended and spear phishing attacks

Why Splunk?

Splunk Enterprise is a real-time data analytics engine that can provide structure for machine data through time-based indexing so that analytics can be applied to the data to gain insight and understanding.

Splunk provides real-time continuous monitoring and trending of FireEye data and supports real-time alerting. This allows Splunk to visualize and express long-term trends that help with prioritization of incident response activities as identified by FireEye. Splunk can ingest tens of terabytes of data per day while monitoring and presenting key performance indicators as configurable dashboards and reports.

Splunk for FireEye—Dashboards and Reports

Splunk generates FireEye dashboards in real-time, which allows for the monitoring of key performance metrics as requested by FireEye customers. Reports from Splunk can be downloaded in PDF or Excel format. Reports can also be scheduled for delivery to individuals as PDFs.

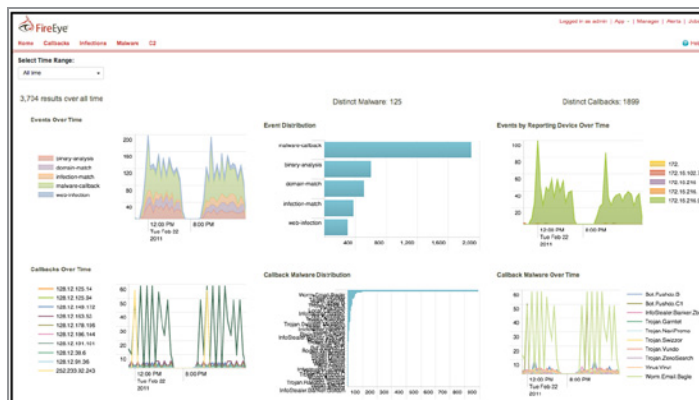
The Splunk App for FireEye supports core Splunk functionality such as role-based access control and drill-down actions that enable you to delve deeper into the details behind graphical elements and charts.

The following reports are available in this version of Splunk for FireEye:

Main FireEye Dashboard provides monitoring for:

- Events by type over time
- Malware distribution by type over the number of systems
- Events by reporting device
- Number of callbacks from specific systems over time
- Number of infected systems by malware type
- Number of callbacks over time by malware name
- Number of inbound infections by host IP over time
- Number of inbound malware infections by name
- Number of inbound malware infections over time by malware name

Malware Callbacks: Callbacks are represented as a table indicating outbound source, number of callbacks, callback destination, callback port, malware name and the first and last times the malware called out.



Callback Drill-downs: Drill-down views contain malware information, transactions, callbacks, trends and correlations. Users can examine a discovered piece of malware in a number of key ways, including:

- Malware – provides an overview of a specific piece of malware including its name, number of callbacks, source and destination, and port and protocol used
- Transactions – provides a view of each of the callbacks as a transaction, identifying the source and destination, the severity and the infection source port
- C2 (callback information) – includes HTTP (layer-7) information along with the URI, HTTP version, user agent (browser version) and the action (GET or PUT)
- Trends – provides an “over-time” graphical view of communication (ports and IPs) between the malware and its call out destination
- Correlation – passes the time of a particular malware activity to Splunk, which launches a search for other activities happening at that same time

Free Download

Download [Splunk](#) for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.