SOLUTION BRIEF

FireEye and Splunk

Better detect, prevent and investigate advanced security threats

SECURITY REIMAGINED

INTEGRATED SOLUTION AT A GLANCE

- **Improve security posture** by finding related malicious activities quickly - use indicators from FireEye malware detection and other security technologies to quickly find related events across the enterprise and over long periods of time
- **Faster security insight** by helping Incident Response team members search, analyze, visualize, collaborate, and report on vast amounts of data
- **Improve analyst efficiency** by providing flexible visualization of data and powerful analytics mechanisms including statistical and correlation capabilities
- Find "**needle in the haystack**" through real-time correlations to identify high-severity events that appear low-level in isolation

FireEye App for Splunk Enterprise allows joint customers to easily correlate and investigate FireEye events across multiple attack vectors. From this one application, users can validate events by pivoting from the Splunk dashboard to obtain supporting artifacts such as PCAPs, disabled malicious binaries, forensic data, and third party lookups.

SPLUNK ENTERPRISE

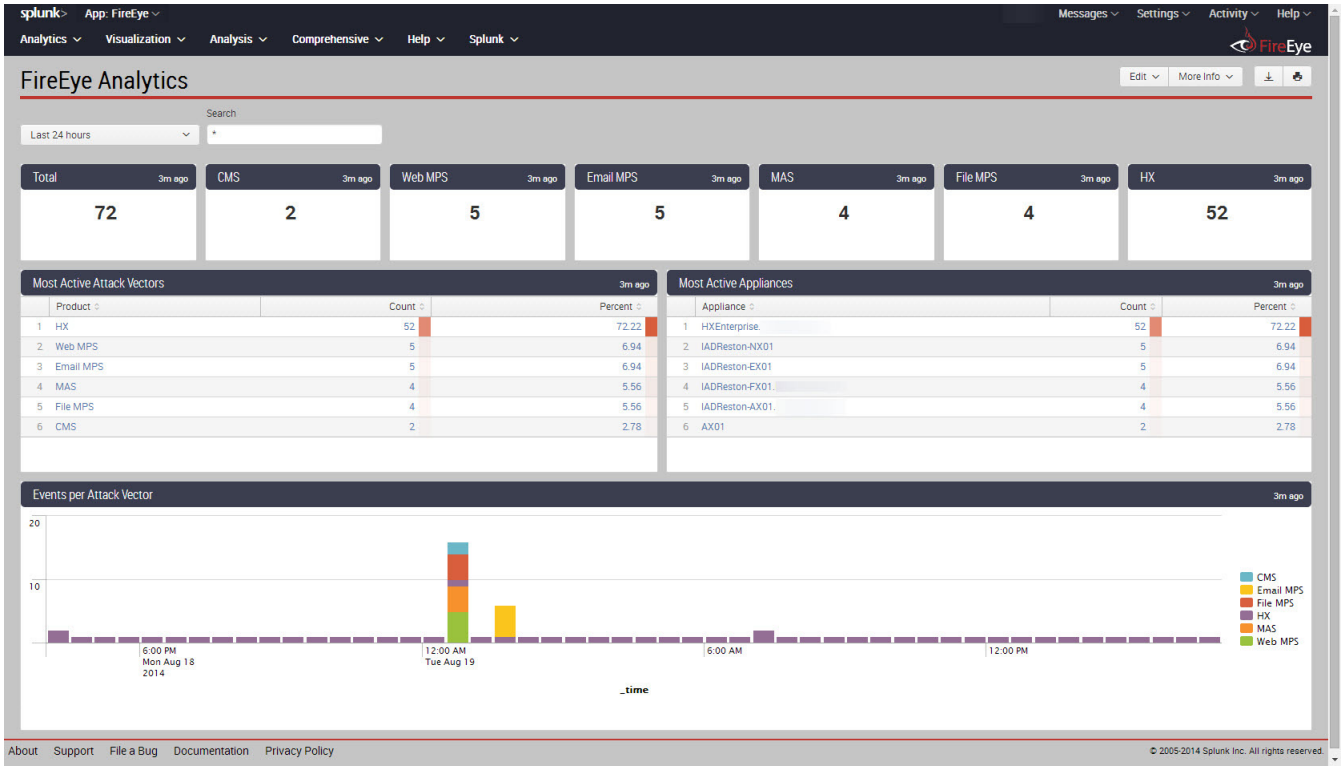
Splunk Provides a Big Data Platform and solutions to collect, index and harness machine-generated data coming from websites, applications, servers, networks and security products, such as FireEye. Splunk solutions such as the Splunk for Enterprise Security are often used as an intelligence platform for security use cases, including security information and event management (SIEM), threat correlation, security reporting and visualization, incident investigations and forensics APT/ malware hunting, and data breach investigations.

HOW THE JOINT SOLUTION WORKS

All FireEye data can be fed into FireEye App for Splunk Enterprise for a holistic view of events and network hygiene. This allows mutual customers to correlate, enrich and look up FireEye data with enterprise context such as user, asset and environment information. In addition, FireEye log and data types have been natively mapped to Splunk's Common Information Model, which further simplifies exposure of FireEye's powerful capabilities.

Splunk-FireEye integration allows FireEye customers to easily visualize key threats as alerted on by FireEye across multiple parameters, investigate FireEye alerts, and see threat trends. Splunk ingests, indexes and analyzes data and events from FireEye, as well as from other data-sources such as IPS, end-points, and firewalls, identity sources, business applications, threat intelligence feeds, asset management databases and other structured or non structured data.

FireEye generates high-fidelity events via threat analysis techniques and multi-vector virtual execution engines, and feeds these events to Splunk to be further correlated and brought in context. Once this data is ingested into Splunk, this application provides first responders the ability to drill down and correlate events by using indicators of compromise such as IP address, alert category, malware URL, hashes, and more.



ABOUT FIREEYE

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 2,500 customers across 65 countries, including over 150 of the Fortune 500.

ABOUT SPLUNK

Splunk Inc. (NASDAQ: SPLK) provides the leading software platform for real-time Operational Intelligence. Splunk® software and cloud services enable organizations to search, monitor, analyze and visualize machine-generated big data coming from websites, applications, servers, networks, sensors and mobile devices. More than 7,000 enterprises, government agencies, universities and service providers in over 90 countries use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, prevent fraud, improve service performance and reduce costs. Splunk products include Splunk® Enterprise, Splunk Cloud™, Splunk Storm®, Hunk™: Splunk Analytics for Hadoop and premium Splunk Apps. To learn more, please visit http://www.splunk.com/company.

FOR MORE INFORMATION, CONTACT ALLIANCES@FIREEYE.COM

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**

FireEye