Advanced Malware Protection for FirePOWER™

BENEFITS

- Continuous detection of malware - immediately and retrospectively
- 'Inline' detection of sophisticated malware that evades traditional network protections
- Combines the world's most effective threat prevention to stop more than just malware
- Easy, integrated managment of malware rules with security policy and access controls
- Lower cost-of-ownership compared to limited-purpose malware appliances
- Optional FireAMP™ protection and remediation solution to extend malware protection to end-devices

Sourcefire® Advanced Malware Protection (AMP) for FirePOWER provides users with the unmatched ability to protect against sophisticated network malware, advanced persistent threats (APTs) and targeted attacks – from point of entry, through propagation, to post-infection remediation. AMP for FirePOWER can be deployed in-line or out-of-band to deliver continuous file analysis and alerting to malware infections. Users gain immediate file disposition and visibility into targeted hosts. AMP for FirePOWER can also retrospectively alert so that users can be notified of malicious files, previously classified as clean or neutral. Deploy as a stand-alone solution or simply software-enable this additional protection when you're ready — with lower cost of ownership than alternatives.

Protection - Before, During And After Attack

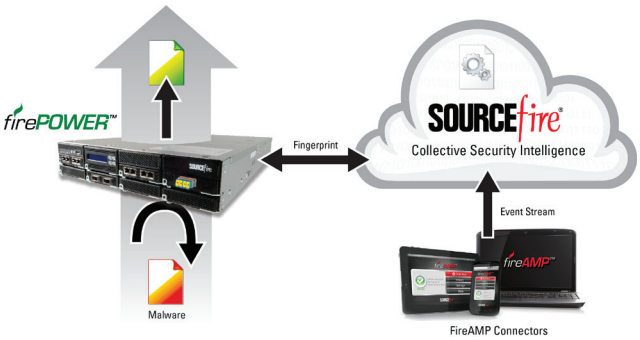
AMP for FirePOWER enables inline malware detection/blocking, continuous analysis, and retrospective alerting and leverages Sourcefire's vast cloud security intelligence. It is a simple subscription add-on to Sourcefire FirePOWER security appliances that enables the following key capabilities:

Inline malware detection/blocking

Identify individual files as they cross the wire, create a fingerprint of each file, check that fingerprint against the Sourcefire collective security intelligence cloud to determine if the file is clean, neutral, or malicious, and take action according to your organization's policies.

Continuous analysis

Analyze a file and track where it goes and how it behaves, even if the file has been previously classified as neutral or clean.



Retrospective alerting

Alert on files previously seen and thought clean or neutral but now, according to the latest threat information and analysis, are identified as malicious. Utilize targeted host and file analysis fingerprint information to speed remediation.

Network File Trajectory

Track malware and suspicious files across the network using existing Sourcefire sensors; providing detailed information on point of entry, propagation, protocols used, and which users or endpoints are involved.

Real-time cloud security intelligence

Leverage Sourcefire Collective Security Intelligence to automatically update blacklists to block communication to malicious sites including not only malware Command and Control servers, but also to spam, phishing, botnet, and open proxies and relay sources.

Complete protection

Deep integration with Sourcefire Next-Generation IPS (NGIPS) and Next-Generation Firewall (NGFW) protects you against all advanced threats that can evade traditional protections. Extend advanced malware protection from the network to end-devices by integrating with Sourcefire FireAMP. Gain greater visibility into malware behavior and trajectory and correlate information to identify and remediate attacks from both perspectives; whether those devices are on or off the corporate network.

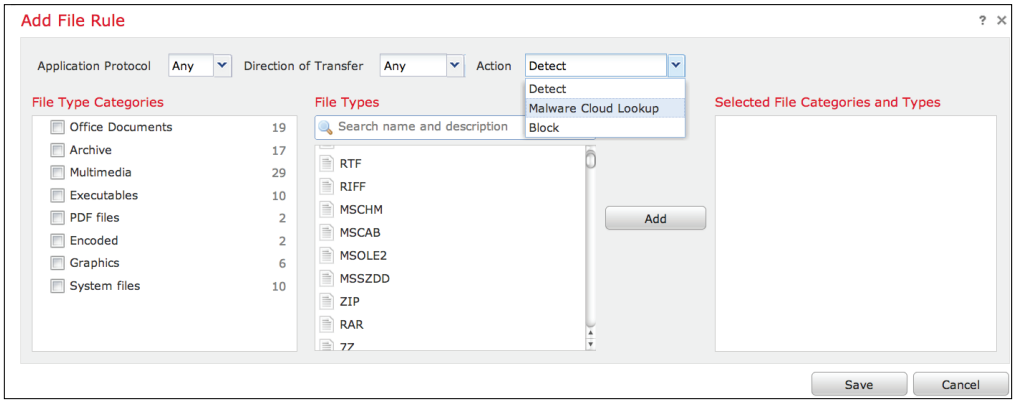


Figure 1. Sourcefire Advanced Malware Protection for FirePOWER is integrated with file type detection to allow granular control and awareness into sophisticated malware for protection before, during, and after the threat.

Lower total cost of ownership

By providing protection for more than just malware, Sourcefire AMP for FirePOWER can save hundreds of thousands of dollars in costs and reduce management complexity over limited-purpose security appliances.

Lower Cost-Of-Ownership Compared To Limited-Purpose Malware Appliances

Expected Three-year Total Cost of Ownership*

There are multiple ways to deploy Sourcefire AMP for FirePOWER to accommodate varying needs:

- **As a subscription license add-on to existing FirePOWER appliances – add protection to your existing Sourcefire NGIPS or NGFW without need for an additional appliance**
- **As a stand-alone appliance solution – provide inline advanced malware protection for your network as an added layer to complement existing security devices**

Either way, you'll be protected by the most cost-effective security solution available today.

*list price (USD) includes appliance, support and subscription costs.

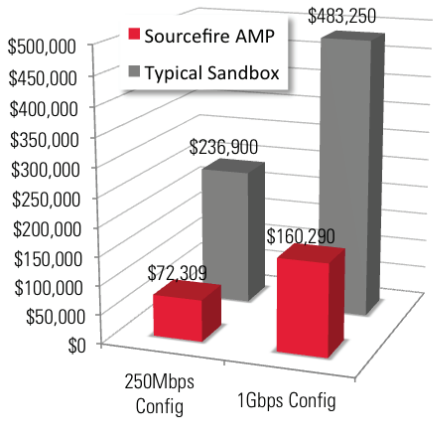


Figure 2. The expected three-year total cost of ownership (TCO) is significantly lower with Sourcefire AMP for FirePOWER versus typical limited-purpose sandbox malware appliances.

"Many CISOs are scrambling to address the insidious threat landscape by implementing Advanced Malware Detection/ Protection technologies as soon as possible. Sourcefire can meet this requirement with both host-based and network safeguards."

- Jon Oltsik, Senior Principal Analyst, ESG Product Brief, November 2012

Added Visibility And Control With FireAMP

FireAMP is Sourcefire's comprehensive advanced malware protection product for PCs, mobile devices, and virtual systems, protecting endpoints whether the devices are connected to a protected network or not. Deployed as a software connector to Sourcefire's sophisticated big data analytics cloud, FireAMP inspects and tracks all file activity on the device to ensure malware is identified prior to infection. Similar to AMP for FirePOWER, in the event malware is identified after-the-fact, FireAMP knows which devices have seen the malware and can target those devices for focused remediation.

Powerful innovations like FireAMP File Trajectory and File Analysis reveal file behaviors, as well as the extent of the outbreak across the network. This enables organizations to identify the initial attack vector for the malware outbreak and the depth and breadth of the infection. FireAMP performs file analysis, detailing

information on how the malware behaves, the parent application, screen shots of the malware executing, and sample packet captures. By providing unmatched visibility regarding the risks to and security posture of an organization, FireAMP helps ensure all instances of a malware infection are identified and cleaned, fully eradicating advanced malware.

Analyzing malware files from 10,000+ organizations around the world, Sourcefire sees emerging malware attacks before widespread infections occur.

"For the past five years, Sourcefire has consistently achieved excellent results in security effectiveness based on our real-world evaluations of exploit evasions, threat block rate and protection capabilities."

- Vikram Phatak, CEO, NSS Labs, Inc.

The World's Most Effective Threat Prevention

Sourcefire provides the best network protection that money can buy — period. Sourcefire is the leader in NSS Lab's Security Value Map for Intrusion Prevention Systems based on security effectiveness and total cost of ownership.[1] As the creator of Snort®, the de facto standard for intrusion detection and prevention, our roots are in security. Our FirePOWER Appliance lineup achieves unprecedented throughput performance, cost-effectiveness and scale. Sourcefire FireSIGHT® increases accuracy and automation by using contextual awareness to understand the composition of your network. This agile engine automatically tunes itself to protect new assets as they enter the network, reducing administrative burden and staying one step ahead of malicious hackers.

Take The Next Steps Toward Agile Security®

To learn more about Sourcefire Advanced Malware Protection and other solutions that provide Agile Security, contact a member of the Sourcefire Global Security Alliance™ today to view a demonstration, request an onsite evaluation, or schedule a meeting, or visit us at sourcefire.com for more information.

Specifications

Advanced Malware Protection for FirePOWER

- Network-based malware protection
- Annual subscription license add-on to FirePOWER appliances – no extra hardware required
- Supported platforms: all FirePOWER 7000 and 8000 Series Appliances and Virtual – VMware 64-bit appliance
- Inspects all or select protocols including http, smtp, imap, pop3
- Inspects inbound, outbound and internal traffic
- Malware lookup for select file types including:
  - Office docs (MSOLE2, XLW, MSWORD_MACS, MDB, ACCDB, MNY, NEW_OFFICE)
  - Archive files (JAR)
  - Multimedia files (SWF)
  - Executables (MSEXE, JARPACK)
  - PDF files (PDF)
- Dispositions for file fingerprint lookups:
  - Clean (file reputation is known good)
  - Neutral (file has unknown reputation or has not been seen before in community)
  - Malicious (file is known to be malicious)
- Actions for file identification:
  - Detect or Block by file type, transfer direction, protocol
  - Malware cloud lookup (malicious files return file SHA256 fingerprint and targeted host IP)
- Prerequisites: requires 5.1.1 or greater Protect License for appliance, Sourcefire Defense Center® (DC) with FireSIGHT, and Sourcefire intelligence cloud connection by DC
- Update frequency: continuously for cloud intelligence lookups (frequently seen file fingerprints are cached locally by DC)

FireAMP Connectors

- Available for the following platforms:
  - Windows XP SP2+
  - Windows Vista SP2+
  - Windows 7
  - Windows Server 2008
  - FireAMP Mobile for Android (v2.2 or greater)
  - FireAMP Virtual for VMware (with EPSEC integration)
- Event integration with DC
- Prerequisites: FireAMP subscription, 5.1 or greater DC with FireSIGHT, Sourcefire intelligence cloud connection
- Connect frequency: continuously for cloud intelligence lookups (frequently seen file fingerprints are cached locally)

4.13 I REV1b