



<http://www.techday.co.nz/itbrief/news/ten-things-you-didnt-know-about-sourcefire/21589/>

Ten things you didn't know about Sourcefire

By Contributor, Friday, 25th November, 2011



1. Headquartered in Columbia, Maryland, Sourcefire was founded in January 2001 by Martin Roesch, author of open-source intrusion detection system [Snort](#).
2. Snort is the world's most widely-deployed intrusion detection and prevention technology, with nearly 4 million downloads to date.
3. In addition to Snort, Sourcefire manages some of the industry's most respected open source security projects, including [ClamAV](#), the most commonly used open source anti-virus and anti-malware gateway product in the world, as well as [Razorbac](#).
4. The company successfully listed for IPO in 2007 and now trades on the NASDAQ Global Select Market under the symbol 'FIRE'.

5. Sourcefire has garnered significant industry recognition, including being named on Forbes' [25 Fastest Growing Technology Companies](#) list earlier this year.

6. Gartner has recognized Sourcefire as a 'leader' in the Gartner Network IPS Magic Quadrant for the fifth consecutive year.

7. Sourcefire holds over 41 patents for innovation and security for customers in over 180 countries.

8. The company offers a range of commercial offerings from Next Gen IPS to consumer endpoints with Immundet, which it purchased in 2010. Immundet, the company's advanced anti-malware solution, has just surpassed 2 million installed endpoints.

9. Sourcefire houses a team called the Vulnerability Research Team (VRT), which is a group of security experts who work around the clock to proactively discover, assess and respond to the latest trends in hacking activities, intrusion attempts and vulnerabilities.

10. Sourcefire products enable the Agile Security vision, which emphasizes the need for more informed, adaptive, and automated security solutions to protect today's dynamic IT environments from constantly changing threats. The vision has four elements:

a) See. Traditional security solutions are mostly blind to their environment and the threats they face. An agile approach provides clarity and vision, reflecting the reality of an environment, as it exists right now.

b) Learn. Applies intelligence to data to improve understanding and decision-making.

c) Adapt. Static approaches limit the ability to tailor protection. Agile Security allows automatic evolution and modification of defenses in response to change.

d) Act. Agile Security provides decisive, flexible and automated responses to events.

Go [here](#) for more on Sourcefire.