

Sourcefire

From Wikipedia, the free encyclopedia

Sourcefire, Inc was a technology company that developed network security hardware and software. The company's Firepower network security appliances are based on Snort, an open-source intrusion detection system (IDS). Sourcefire was acquired by Cisco for \$2.7 billion in July 2013.^{[1][2]}

Contents

- 1 Background
- 2 Financial
- 3 Products
 - 3.1 Firepower
 - 3.2 Advanced Malware Protection
 - 3.3 Snort
 - 3.4 Immundet
- 4 See also
- 5 Notes
- 6 References
- 7 External links

Background

Sourcefire was founded in 2001 by Martin Roesch, the creator of Snort. The company created a commercial version of the Snort software, the Sourcefire 3D System, which evolved into the company's Firepower line of network security products. The company's headquarters was in Columbia, Maryland in the United States, with offices abroad.

Financial

The company's initial growth was funded through four separate rounds of financing raising a total of \$56.5 million from venture investors such as Sierra Ventures, New Enterprise Associates, Sequoia Capital, Core Capital Partners, Inflection Point Ventures, Meritech Capital Partners, and Cross Creek Capital, L.P.^[a]

In 2005, Check Point Software attempted to acquire Sourcefire for \$225 million,^[3] but later withdrew its offer after it became clear US authorities would attempt to block the acquisition.^[4] The company completed an initial public offering in March 2007, raising \$86.3 million.^{[5][b]} In August of the same year, Sourcefire acquired Clam AntiVirus.^[6] Sourcefire rejected an offer of \$187 million in May 2008 from security appliance vendor Barracuda Networks,^[7] who had offered to pay US\$7.50 per share, amounting to a 13% premium of their then-current stock price.^[8] Sourcefire announced its acquisition of the cloud-based antivirus firm Immundet in January 2011.^{[9][10]}

Revenue for the fourth quarter of 2012 was \$67.4 million compared to \$53.2 million in the fourth quarter of 2011, an increase of 27%.^[11] Revenue for the year ending December 31, 2012 was \$223.1 million compared to \$165.6 million for 2011, an increase of 35%. International revenues were \$74.4 million, up 77% over 2011. As

Sourcefire



Type	Subsidiary
Industry	Network security; intrusion detection, intrusion prevention system and anti-malware
Fate	Acquired
Founded	2001
Founder	Martin Roesch
Headquarters	Columbia, Maryland
Key people	John Becker (CEO), Martin Roesch (Founder and CTO)
Products	Sourcefire Firepower network security appliances
Revenue	\$223.1M (FY12)
Number of employees	560 (3Q12)
Parent	Cisco Systems
Website	sourcefire.com (http://sourcefire.com/)

of December 31, 2012, the company's cash, cash equivalents, and investments totaled \$204.0 million.^[12]

Sourcefire received SC Magazine's 2009 "Reader Trust" award for best intrusion detection and intrusion prevention system (IDS/IPS) for Snort^[13] and Network World's "2009 Best of Tests" award for the Sourcefire 3D System.^[14] The company placed in the "Leaders" Quadrant in the 2012 Gartner Magic Quadrant competition for intrusion detection and prevention system appliances,^[15] and received ICSA Labs' certification for the full line of Firepower (formerly 3D) appliances.^[16] Sourcefire was given a top "recommend" rating in 2012 for fastest and most accurate IPS detection from NSS Labs.^[17] Firepower was also ranked by NSS Labs at the top of their 2012 "Security Value Map" in security effectiveness and total cost of ownership.^[18]

On July 23, 2013, Cisco Systems announced a definitive agreement to acquire Sourcefire for \$2.7 billion.^{[1][19]}

Products

Firepower

The Sourcefire Firepower line of appliances are designed to form part of a layered security defense. They can be deployed as:

- Next-Generation Intrusion Prevention System (NGIPS), with network visibility into hosts, operating systems, applications, services, protocols, users, content, network behavior and network attacks and malware.
- Next-Generation Firewall (NGFW) with NGIPS, incorporating access and application control, threat prevention and firewall capabilities
- Next-Generation Intrusion Prevention System with integrated:
 - Application control
 - Malware protection
 - URL filtering
- Advanced Malware Protection Appliance for dedicated inline network protection against advanced malware.

Advanced Malware Protection

Sourcefire Advanced Malware Protection (AMP) offers malware analysis and protection for networks and endpoints using big data analytics to discover, understand and block advanced malware outbreaks, advanced persistent threats (APTs) and targeted attacks. AMP enables malware detection and blocking while provisioning continuous analysis and retrospective alerting, using Sourcefire's cloud security intelligence.

Advanced Malware Protection can be deployed inline via a product key on NGIPS, dedicated AMP Firepower appliance or on endpoints, virtual and mobile devices with FireAMP.^[20]

Snort

Snort is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines signature, protocol and anomaly based inspection methods. Developed in tandem with the Snort open source community, its developers claim it is the most widely deployed intrusion detection and prevention technology worldwide.^[21]

Immunet

Immunet uses the cloud virus definitions along with virus definitions from Clam AntiVirus which is an open source (GPL) anti-virus toolkit primarily used on UNIX operating systems designed for e-mail scanning on e-mail gateways. It provides a number of utilities including a multi-threaded daemon, a command-line interface scanner and tool for automatic database updates. The core of the package is an anti-virus engine available in a form of a shared library.^[22] Immunet is provided in two versions, Free and Plus.^[23]

As of June 10, 2014, Immunet Plus is no longer available, replaced with Immunet Free, supported by Cisco.^[8]

See also

- Antivirus software
- Intrusion detection system (IDS)
- Real-time adaptive security
- Sourcefire Vulnerability Research Team

Notes

- a. A venture fund whose general partner is a wholly owned subsidiary of Wasatch Advisors, Inc.
- b. The sole book-running manager of the offering was Morgan Stanley & Co. Incorporated. Lehman Brothers Inc. acted as co-lead manager and UBS Securities LLC and Jefferies Group LLC served as co-managers.

References

1. "Cisco Completes Acquisition of Sourcefire". Cisco Systems. October 7, 2013. Retrieved October 7, 2013.
2. "Cisco to Buy Sourcefire, a Cybersecurity Company, for \$2.7 Billion". *The New York Times*. July 23, 2013. Retrieved July 23, 2013.
3. "Check Point and Sourcefire to Explore Alternative Business Relationship". Check Point. March 23, 2006. Archived from the original on March 26, 2014. Retrieved October 12, 2008.
4. "Check Point calls off Sourcefire buy". Symantec. March 24, 2006. Retrieved October 13, 2008.
5. "Top 10 technology IPOs of 2007". *TechTarget*. December 31, 2007. Retrieved September 24, 2016.
6. "Sourcefire acquires ClamAV". SecurityFocus. August 17, 2007. Retrieved October 28, 2008.
7. "Barracuda hungry for OSS security developer Sourcefire". *Ars Technica*. May 30, 2008. Retrieved August 20, 2009.
8. "Sourcefire says no to Barracuda's takeover bid". *Infoworld*. May 30, 2008. Retrieved August 20, 2009.
9. Friedrichs, Oliver. "Immunet Acquired by Sourcefire". Immunet. Archived from the original on April 10, 2011. Retrieved April 10, 2011.
10. "Sourcefire Announces Acquisition of Immunet". Sourcefire. Business Wire. January 5, 2011. Archived from the original on April 10, 2011. Retrieved April 10, 2011.
11. "Sourcefire Security Blazes Up on Q4 After VMware Drop". *Investor's Business Daily*. February 22, 2013. Retrieved September 24, 2016. (subscription required (help)).
12. "Sourcefire Announces Record Revenue for Fourth Quarter & Full Year 2012". Yahoo! Finance. Marketwire. February 21, 2013. Retrieved February 21, 2013.
13. "Best IDS/IPS solution". *SC Magazine*. Haymarket Media Group. April 22, 2009. Archived from the original on November 27, 2011. Retrieved October 29, 2009.
14. "2009 Best of the Tests winners". *Network World*. February 24, 2009. Retrieved October 29, 2009.
15. "Gartner Magic Quadrant Report". Gartner. July 5, 2012. Archived from the original on October 23, 2013. Retrieved December 26, 2012.
16. "ICSA Labs Report" (PDF). International Computer Security Association. September 21, 2009. Retrieved October 29, 2009.
17. "NSS Labs Security Value Map for Intrusion Prevention Systems". Sourcefire. Business Wire. January 30, 2013. Archived from the original on February 13, 2013. Retrieved January 30, 2013.
18. "2012 Intrusion Prevention Systems Security Value Map" (PDF). NSS Labs. August 31, 2012. Archived from the original (PDF) on February 13, 2013. Retrieved August 31, 2012.
19. "Cisco Agrees to Buy Sourcefire in \$2.7 Billion Deal". Bloomberg News. July 23, 2013. Retrieved September 25, 2016.
20. "FireAMP Fights Malware with Big Data Analytics". *PC World*. January 23, 2012. Retrieved January 23, 2012.
21. "Snort Website". Retrieved October 28, 2008.
22. "ClamAV Website". Archived from the original on January 10, 2010. Retrieved October 28, 2008.