



What is ClamAV?

Clam AV is a leading open source gateway anti-virus and anti-malware project. It provides a number of utilities including a flexible and scalable multi-threaded daemon, a command line scanner and an advanced tool for automatic virus signature updates.

For more information about ClamAV, visit www.clamav.org.

How does ClamAV compare to commercial anti-virus solutions?

As an open source project, hundreds if not thousands of individuals have inspected the ClamAV source code and contributed to the overall quality and stability of the code as well as the vast library of ClamAV malware signatures. ClamAV is comparable in quality and coverage to leading commercial anti-virus solutions and was recently named a finalist in the “Best Tool or Utility for SysAdmins” at the Sourceforge.net 2007 Community Choice Awards.

At LinuxWorld this year, ClamAV was one of only three antivirus products to provide a 100% detection rate in their live ‘Fight Club’ test featuring live submissions from the show audience. One vendor caught fewer than 10 percent! The full article is available at:

http://www.darkreading.com/document.asp?doc_id=131246&WT.svl=news1_1

How big is ClamAV?

ClamAV one of the most broadly adopted open source security projects worldwide:

- Nearly 1 million unique IP addresses download ClamAV malware updates daily.
- ClamAV is a truly global project with more than 120 mirrors in 38 countries.
- Network security solution and service providers worldwide have adopted ClamAV.

Where is ClamAV based?

The core ClamAV team is a distributed organization based in Poland, the UK, Germany and Italy. Contributors to ClamAV malware updates are located around the world.

What, exactly, is Sourcefire acquiring?

Sourcefire has acquired the ClamAV project and related trademarks, as well as the copyrights held by the five principal members of the ClamAV team including project founder Tomasz Kojm. Sourcefire will also assume control of the open source ClamAV project including the ClamAV.org domain, web site and web site content and the ClamAV Sourceforge project page.

Why did Sourcefire acquire ClamAV? Is Sourcefire entering the anti-virus market?

Many critical market segments depend on ClamAV’s ability to identify deeply embedded threats, such as viruses, spyware and other forms of malware. These include:

- Unified Threat Management (UTM) Systems
- Secure Web Gateways
- Secure Mail Gateway

These categories of solutions are potential logical extensions of Sourcefire’s comprehensive Enterprise Threat Management (ETM) strategy.

When is the transaction effective?

The acquisition has closed and is effective immediately.

What was the purchase price?

The terms of the purchase have not been disclosed.

When will Sourcefire begin to integrate ClamAV technology into its products?

Sourcefire intends to offer support and training services to ClamAV users beginning in Q4 2007. We anticipate offering products based on ClamAV as a part of our Enterprise Threat Management product family in the latter half of 2008.

Will the ClamAV team be joining Sourcefire?

Yes, all of the core ClamAV team will join Sourcefire as permanent employees. They are: Tomasz Kojm, Cristoph Cordes, Nigel Horne, Luca Gibelli and Alberto Wu.

Who will maintain daily updates to the ClamAV malware database?

The ClamAV malware database contains over 145,000 signatures. ClamAV will remain an open source (GPL) project with dozens of individuals from the ClamAV community contributing daily signature updates, including the core ClamAV team that will now become part of the Sourcefire product development team.

What are the key capabilities of ClamAV?

ClamAV offers the following capabilities and attributes:

- Command-line scanner
- Virus database with over 145,000 signatures updated multiple times per day
- Fast, multi-threaded daemon with support for on-access scanning
- Milter interface for sendmail
- Advanced database updater with support for scripted updates and digital signatures
- Virus scanner C library
- Built-in support for various archive formats, including Zip, RAR, Tar, Gzip, Bzip2, OLE2, Cabinet, CHM, BinHex, SIS and others
- Built-in support for almost all mail file formats
- Built-in support for ELF executables and Portable Executable files compressed with UPX, FSG, Petite, NsPack, wwpack32, MEW, Upack and obfuscated with SUE, Y0da Cryptor and others
- Built-in support for popular document formats including MS Office and MacOffice files, HTML, RTF and PDF

Will Sourcefire change the way that ClamAV open source software is offered?

Sourcefire has no current plans to change the way the ClamAV software is offered to end-users. Sourcefire is committed to investing in and advancing the ClamAV technology, just as we have with Snort and Snort.org. Sourcefire is absolutely committed to the continued distribution of ClamAV and the ClamAV malware database as an open source solution under the terms of the GPL.