

Metascan® Custom Packages

Next-Generation Static File Analysis Solutions

10GB

Metascan[®] Custom Packages

Metascan is an automated static file analysis solution used to quickly, efficiently and systematically analyze files and detect the presence of malicious applications by using many tightly integrated antivirus engines.

Key Benefits

- Quickly test for the existence of malware using multiple scanning engines, freeing up valuable time usually spent manually scanning files
- Antivirus engine licensing is included so there is no need to purchase and manage licenses
- A web interface allows anyone with a web browser to quickly scan a static file to determine its status, as well as threat information if any are detected (class of malware, threat name, engines that detected the threat)
- Can be quickly integrated into an organization's workflow allowing for threat and risk mitigation in a relatively short period of time

With the latest tally of malware at over 50 million unique samples, fast and automated analysis of threats is absolutely necessary. Researchers cannot always submit files to public services due to the sensitive nature of some of their samples. The Metascan appliance is truly a plug-and-play solution that quickly tests for the existence of malware using a multitude of scanning engines. Packaged as a ready-to-run appliance, Metascan can be quickly integrated into an organization's workflow. Metascan is a high performance file analysis solution that provides a database, web based GUI, and other features such as the ability to connect to multiple Metascan servers for unprecedented scalability in anti-malware scanning capabilities.

Packaging Options

Pre-configured Appliance

A true plug-and-play solution with pre-configured and fully-licensed AV engines.

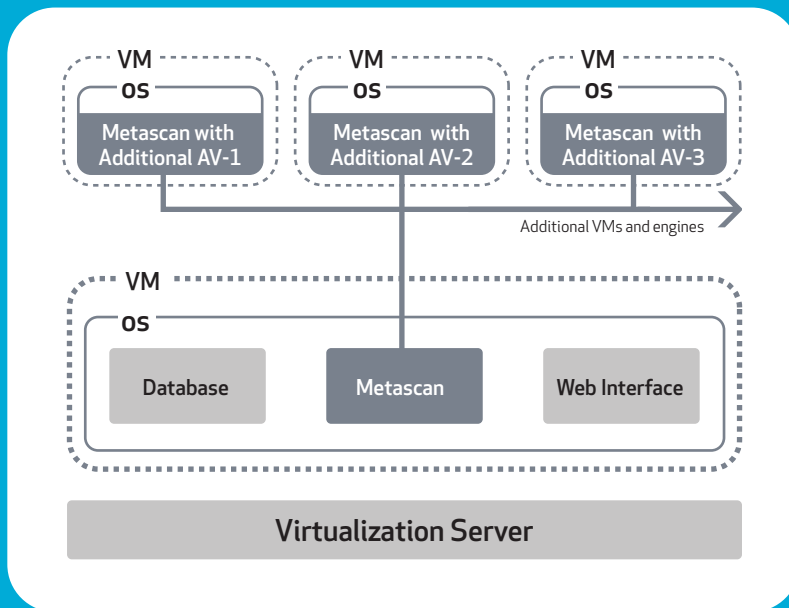
Downloadable Software

Metascan can be installed on your own appliance or VM. OPSWAT Professional Services can assist with the installation and configuration.

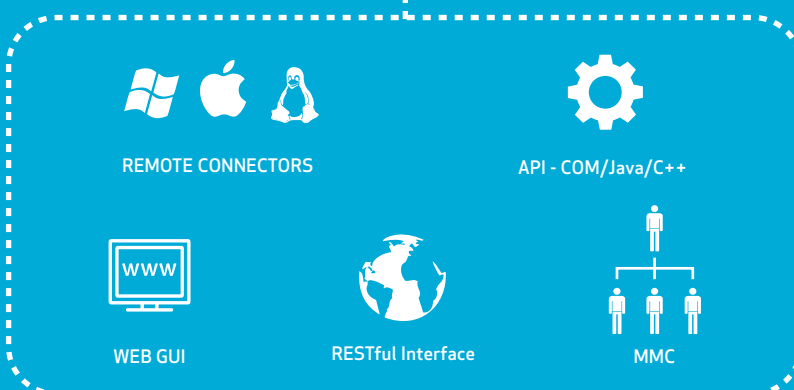
Custom Engine Packages

Want a custom Metascan configuration with 10, 20, 30 or any other set of engines? Contact sales@opswat.com and allow us to tailor a solution per your organization's unique needs.

Example Metascan System Architecture



Metascan Server



CONNECTIVITY METHODS

Features

- Scalable modular architecture for large-scale parallel file analysis operations
- Easy integration with existing sandbox solutions such as Norman and GFI
- Secure RAM drive for the deletion of confidential data (i.e. system failure or restart)
- Standards-compliant Web interface
- Scan individual files or complete folders
- Analysis reports such as individual and total scan engine detection times
- Custom reports are available via downloadable CSV files
- Microsoft Management Console (MMC) Snap-In for local management and additional functionality
- Automated updating of all antivirus engines (for off-line systems, manual updates are supported for Metascan embedded engines)
- Search via threat name, MD5 or SHA1 hashes
- APIs for custom integration (RESTful, Java (JNI), COM for Visual Basic and C#, ICAP and C++)
- Custom scanning engine support
- Built-in file type detection for over 5,000 file types - including archives (Winzip, WinRar, PKZip and other types of archive files)
- Post actions allow users to create and implement custom scripts that are executed after completing a file scan

Metascan[®] Custom Packages

Online Demo

A free, online demonstration of Metascan functionality is available at: www.metascan-online.com

File Browser

The file browser displays all files scanned through Metascan, as well as provides an in-depth view of each scan's results.

Uploaded	Last Scanned	Filename	Scan Result
2011-02-03 15:19:18	2011-02-03 15:19:18	Citrix4.customscan.cab	CLEAN
2011-02-03 13:47:53	2011-02-03 13:47:53	loading.gif	CLEAN
2011-02-01 18:35:02	2011-02-01 18:35:02	scanme2.pdf	INFECTED
2011-02-02 10:48:50	2011-02-02 10:48:50	XP SP3 English 100GB HD-2011-02-02-10-08-53.png	CLEAN
2011-02-02 08:34:15	2011-02-02 08:34:15	report.csv	CLEAN
2011-02-02 07:48:58	2011-02-02 07:48:58	jira-soapclient-1.1-src.tar.gz	CLEAN
2011-02-01 18:38:15	2011-02-01 18:38:15	jre-6u23-windows-i586-iftw.pdf	CLEAN
2011-02-01 18:36:58	2011-02-01 18:36:58	OLLYDBG - Copy.EXE	CLEAN
2011-02-02 12:03:09	2011-02-02 12:03:09	Windows_AVSDK_Support_Chart_3_4_21_0.xml	CLEAN
2011-02-01 18:32:44	2011-02-01 18:32:44	scanme.pdf	CLEAN
2011-02-01 11:13:51	2011-02-01 11:13:51	agbinst.exe	CLEAN
2011-01-31 16:49:32	2011-01-31 16:49:32	clamwin-0.96.5-setup.exe	CLEAN
2011-01-31 13:45:45	2011-01-31 13:45:45	Metascan_Core_3_1_2_8740.msi	CLEAN
2011-01-31 13:29:22	2011-01-31 13:29:22	SpecialCharViruses.rar	CLEAN
2011-01-31 13:27:17	2011-01-31 13:27:17	XP SP3 English 100GB HD-2011-01-18-15-13-51.png	CLEAN
2011-01-31 13:18:24	2011-01-31 13:18:24	XP SP3 English 100GB HD-2011-01-25-11-16-38.png	CLEAN
2011-01-31 12:17:19	2011-01-31 12:17:19	Setup.exe	CLEAN
2011-01-31 12:00:05	2011-01-31 12:00:05	AdobeOwlCanvas.dll	CLEAN
2011-01-31 11:56:27	2011-01-31 11:56:27	Photoshop.dll	CLEAN

scanme2.pdf uploaded on 2011-02-02 02:35:02 AM UTC

Uploaded: 2011-02-02 02:35:02 AM UTC
Last Scanned: 2011-02-02 02:35:20 AM UTC
Filename: scanme2.pdf (1286517 bytes)
Scan Time: 14.375 secs.
MD5: 84d215bf266ee979bf52c34f5f9bff3a
SHA1: a89a7f196f4218ebd2985d8079dd90decfed9a7e
Detected Type: data
Result: **INFECTED (14.3% detection rate)**

Engine	Scan Time (ms)	Def Date	Result
avast! Antivirus Professional	1406	2011-02-01 00:00:00	CLEAN
avast! Pro Antivirus	1297	2011-01-31 00:00:00	CLEAN
AVG scan engine	31	2011-01-31 00:00:00	CLEAN
Avira AntiVir Premium	14375	2011-02-01 00:00:00	CLEAN
BitDefender Antivirus 2010	3734	2011-01-26 00:00:00	INFECTED
BullGuard 9.0	4219	2011-02-02 00:00:00	INFECTED
CA scan engine	16	2011-01-30 00:00:00	CLEAN
ClamWin scan engine	672	2011-01-31 00:00:00	CLEAN
Emsisoft Anti-Malware	1906	2010-10-07 00:00:00	CLEAN
ESET scan engine	16	2011-01-31 00:00:00	CLEAN
F-PROT Antivirus for Windows	2953	2011-02-01 00:00:00	CLEAN
F-Secure Anti-Virus	4594	2011-02-02 00:00:00	INFECTED

Contact Information

OPSWAT, Inc.
640 2nd Street, 2nd Floor
San Francisco, CA 94107

415.543.1534 sales
sales@opswat.com
www.opswat.com



ISV/Software Solutions