

CONTENT VERIFICATION SUITE

FILE TYPE CONTENT ANALYSIS WITH CONFIGURABLE POLICY ENFORCEMENT

/// FACT SHEET



The EDS Content Verification Suite has been developed to meet the emerging security needs for content type enforcement. Flexibility, extensibility and environment integration are key architectural features. Aimed to meet the security requirements of a market which demands the highest levels of security and integrity.

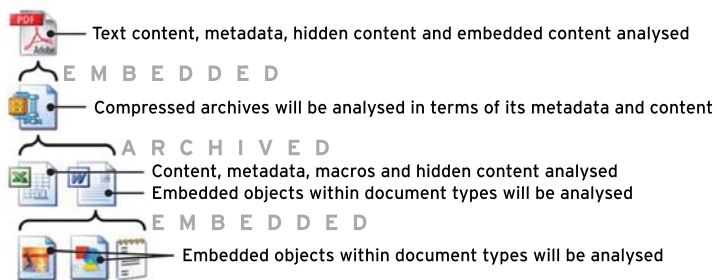
KEY COMPONENTS

- Extensible architecture allowing new file type and text scanning filters.
- GUI Based Policy Editor.
- Third part integration:
 - EDS Multi-Protocol Gateway.
 - Microsoft Internet Security and Acceleration Server.
 - OEM SDK
- Command Line based scanner for Microsoft Windows (2000/XP/2003/Vista)
- Bespoke file signature checking algorithms providing recursive processing.
- Comprehensive file type support out of the box.
- Script detection.
- Comprehensive auditing.

Overview

The EDS CV Suite technology offers an extensible framework architecture which provides an enablement platform for bespoke filter development. This provides support for the ever changing needs of this fast growing sector of the security market.

The EDS CV capability is ideally placed for both specialist niche scenarios as well as wider market opportunities. Focused, and deployed initially in the UK Defence marketplace, the technology seeks to track upcoming standards of CV product assurance from UK government security and information assurance agencies.



The CV Suite's out of the box support and adaptability means the technology is deployable in a wide spectrum of markets, including: military, government, financial and commercial sectors.

Threats

- Accidental confidential information leakage
- Metadata leakage
- Unauthorized export of confidential information
- Skilled engineering attacks using file impersonation (masquerading files)
- Malicious scripting

FEATURES

- Enforces content security policy at the network boundary or at the desktop.
- Does not require additional applications to be installed, such as Microsoft Office or Adobe Acrobat.

SYSTEM REQUIREMENTS

- Windows Operating System (2000/XP/2003/Vista)

FUTURE CAPABILITY

- Macro detection.
- Steganography analysis.
- Metadata detection.
- Hidden content detection.
- Vocabulary based analysis.
- Microsoft Exchange integration.
- Integrated COTS Antivirus integration.

POINT OF CONTACT

Chris Abbott

CBRN Business Relationship Manager

T: +44 (0)1256 742043

F: +44 (0)1256 742480

E: chris.abbott@d.edl.uk.eds.com

The Content Verification Suite is used within the EDS Multi-Protocol Gateway to offer enhanced policy enforcement over many protocols, such as: X.400, SMTP (MIME/SMIME), ACPI45, STANAG 4406 and FTP.

Many file types offer the ability to attach or embed content within themselves; typically this is seen with archive based file formats but is also possible within document formats such as PDF. Compound Documents are a prime example of this and the best examples can be seen in the Microsoft Office family of products.

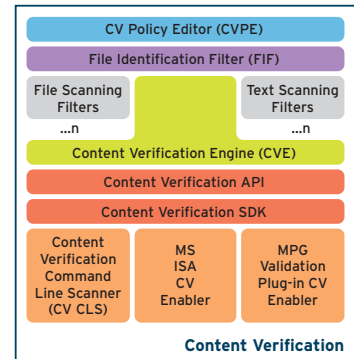
These file formats allow other files, and object types, to be embedded within a root storage document. The Content Verifier must ensure that each embedded object is permitted within the parent document and is in turn permitted in-line with the current configuration policy in force.

The Content Verification scan engine is a fully recursive checker which can scan within compound documents, and other supported file types which enable attachment and embedding of other content.

The framework is fully customisable and allows custom filters to be added for file and text based scanning.



Name	Description	File Extension
CSV	Comma Separated Values (CSV) file	csv
MSAccess	Microsoft Access Database	mdb
Acrobat	Adobe Acrobat - Portable Document Format Document	pdf
Bitmap	Windows Bitmap	bmp,dib
MSExcel	Microsoft Excel Document	xls
Executable	Executable Content	exe,com,dll
GIF	Graphic Interchange Format (GIF)	gif
JPEG	Joint Photographic Expert Group (JPEG) Graphic	jpg,jpeg,jpe
MSGMessage	Microsoft Message File	msg
MSPresent	Microsoft Project	mpp
MSPowerpoint	Microsoft Powerpoint Document	ppt,pptx
RichText	Rich Text Format Document	rtf
Text	Text Document	txt
TIFF	Tag Image File Format (TIFF)	tif
Microsoft Word	Microsoft Word Document	doc
Zip	PKZIP Compatible Compressed Files	zip
AdobePS	Adobe Encapsulated Postscript File	eps
Avi	Audio Video Interleave (AVI)	avi
CSS	Cascading Style Sheet	css
HTML	Hyper Text Markup Language (HTML)	htm,html
MP3	MP3 Audio File	mp3
MPEG	Moving Picture Expert Group (MPEG) Video File	mpeg,mpeg
MSWord	Microsoft Word File	doc
PNG	Portable Network Graphics File	png
QuickTime	QuickTime Movie	mov



The Content Verification engine enforces a configurable policy file which offers fine grained control. It is possible to configure which file types are to be allowed and disallowed as well as offering the ability to configure which types should be permitted within other types.

Settings also exist for enhanced configurability. Examples of this are options for maximum compression ratios on archives, maximum message body for email and the maximum file recursion depth before a file is considered malicious.

The CV engine will fail safe and block any content that it cannot determine or is not configured within the policy file.

Contact

EDS Defence, 1-3 Bartley Wood Business Park
Bartley Way, Hook, Hampshire RG27 9XA
phone: +44 (0)1256 742000
fax: +44 (0)1256 742612
visit: www.edsdefence.com
visit: www.eds.com



EXPERTISE. ANSWERS. RESULTS.