

## ICAP for AVIRA SAVAPI

Local scan engine for  
Internet traffic and HTTP proxy

# ICAP

**Avira's ICAP server** delivers the industry's best malware protection for your customers' web based traffic. The Avira ICAP server includes the SAVAPI SDK and is an ideal technology for those vendors looking to build their own branded solution without the burden of having to undertake low level integration. It works seamlessly with SQUID and other ICAP clients.

Ideal for integration in complex security solutions such as Unified Threat Management, Next Generation Firewall or web filtering solutions the ICAP server provides you with the ability to filter or scan files to/from the Internet. Delivered as a binary package, it enables integration by simply configuring the ICAP port and the license file.



### KEY FEATURES:

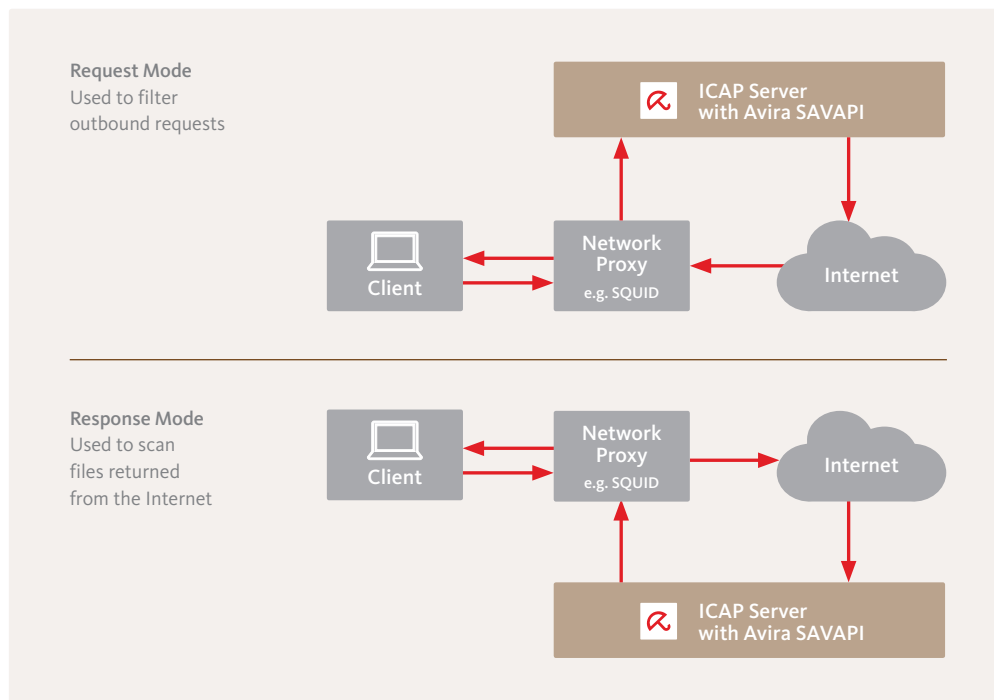
- Runs on all major Linux distributions (Redhat, Ubuntu, Suse, Debian)
- Runs on Intel compatible processors
- Highly customizable templates to allow branding
- Fully compatible with SQUID and many other ICAP Clients
- Designed for high performance, reliability, and low resource usage
- Capable of filtering on file extension and requested content type
- Multi-threading ready
- Multi-processing ready
- Own licensing mechanism
- Own updater with HTTPS Support and without service interruption

## Application

ICAP Server with SAVAPI SDK operates in a Request or Response mode, depending on whether filtering, or scanning, of files is required.

In Request mode, traffic from a client is routed by the proxy to the ICAP server which applies policies to filter the traffic based on a number of criteria including file extension or content type (application / executable / streaming traffic).

In Response mode, the ICAP server scans the file presented in the return path for malware, before it is delivered to the client.



## Specifications

- **Size:**  
> 250MB
- **Supported OS / Hardware:**  
Linux / Intel
- **Implementation:**  
Daemon
- **Functionality:**  
99.9% Detection rate  
Generic and heuristic  
Advanced archive scanner  
Interfaces with Avira Protection Cloud
- **Scan and Detection:**  
Malicious Windows .exe / .dll  
Linux, MacOS and Android malware  
Malicious script: JavaScript, VBScript etc  
Office docs and embedded macros
- **Unarchiving:**  
All known archives  
Flag password protected archives
- **Decoders:**  
MBOX, MIME attachments
- **Adware and Spyware (selection):**  
Worms, mailers  
Web-based malware  
(HTML, JavaScript, VBS)  
Script virus DOS Batch MIRC/ IRC script  
Shell script (Bash etc.)  
PIF, INI, REG (ASCII)
- **Viruses (selection):**  
Encrypters, Polymorphic & Metamorphic viruses  
Stealth viruses, Boot /File/MultiPartite  
Java Applets, Exploits in file formats.  
SPR (Security Privacy Risk e.g.: Jokes)

## Contact Avira

### Europe, Middle East, Africa

Avira  
Kaplaneiweg 1  
88069 Tettngang | Germany  
Tel: +49 7542 5000  
Email: oem@avira.com

### Americas

Avira, Inc.  
330 Primrose Rd. | Suite 610  
Burlingame | CA 94010 | USA  
Tel: (800) 403-5207  
Email: oem@avira.com

### Asia / Pacific and China

Avira (Representative Office)  
10 Anson Road  
23-11/12 International Plaza  
Singapore 079903  
Email: oem@avira.com