

US 8,677,494

Avast Software("Avast")

For purposes of this chart, the licensed Avast products include Endpoint Protection and other antivirus products utilizing Avast! Research Labs, DynaGen, Malware Similarity Search, and Evo-Gen technologies.

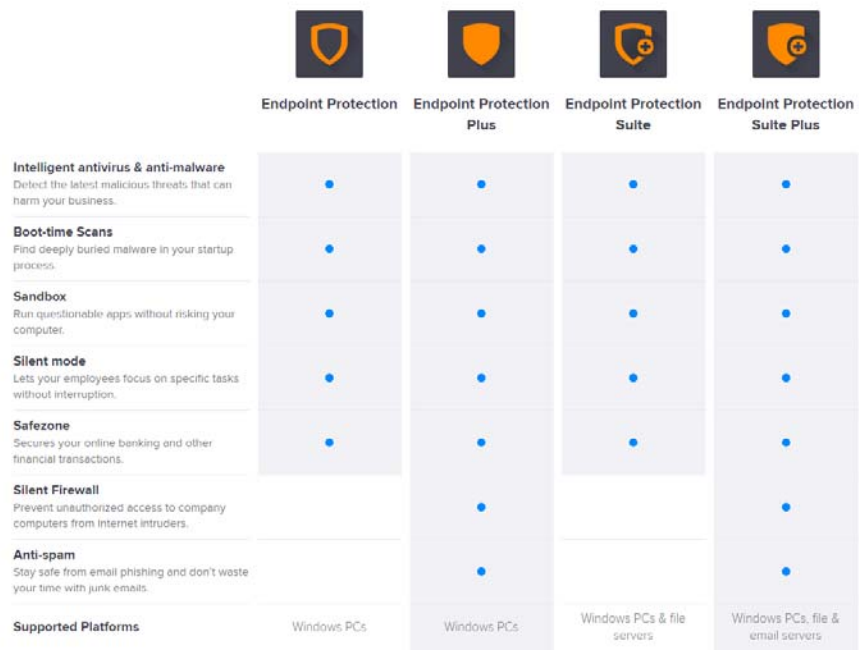
As identified and described element by element below, the licensed products specifically listed above meet at least claim 1 of the '494 Patent.

Claim 1

1a. A computer based method, comprising the steps of:

Avast's products meet the recited claim language because it receives an incoming downloadable.

Avast products, including Endpoint Protection, are software based products that use computer processors for scanning incoming program code, or executable files, data, and other content they receive, performing analysis including sandboxing, creating a profile of the incoming downloadable and sending the information gathered to be stored in a database.



<https://www.avast.com/en-us/business>

1b. receiving an incoming downloadable

Avast's products meet the recited claim language because they receive incoming downloadables.

As shown below, Avast's Endpoint Protection and other antivirus software meet the recited claim language. The avast! Research Lab uses DynaGen technology to classify files as clean or dirty and create generic malware descriptions from multiple dirty files having shared characteristics. avast! 2014 Frequently Asked Questions -- New Features < http://www.avast.com/en-us/faq.php?article=AVKB89#idt_01 >; avast! antivirus: security from cloud (2013) at pp. 15-18; New Toy in the Avast Research Lab (2012) < <http://blog.avast.com/2012/12/03/new-toy-research-lab/> >; Declaring machine

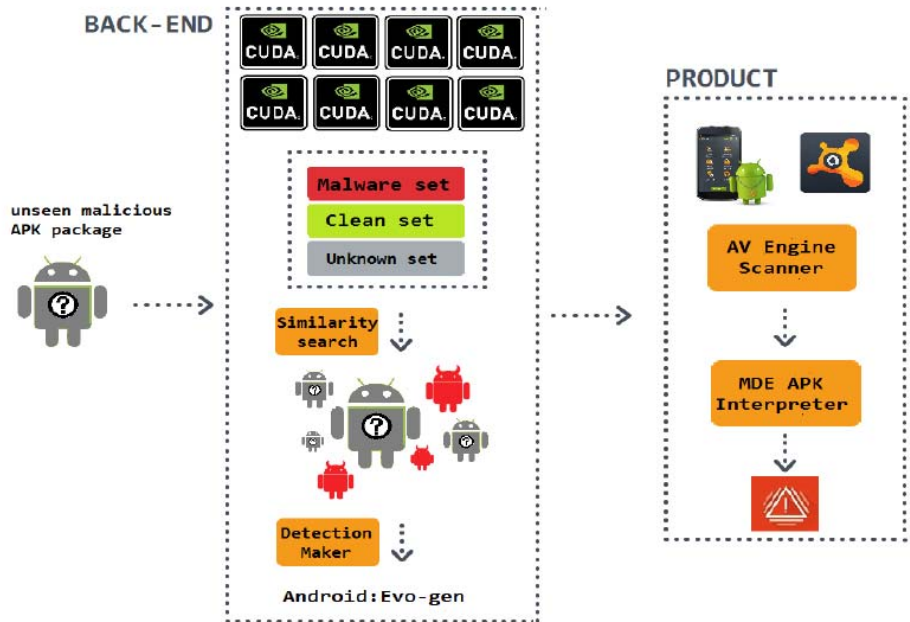
war against malicious Android packages (2014) < <http://blog.avast.com/2014/04/02/declaring-machine-war-against-malicious-android-packages/> >.

The files analyzed by DynaGen include unclassified executable files that are downloaded over the Internet to endpoints running avast! endpoint security software, and then received from the endpoints to the avast! Research Lab for "back-end" analysis.

1c. deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and

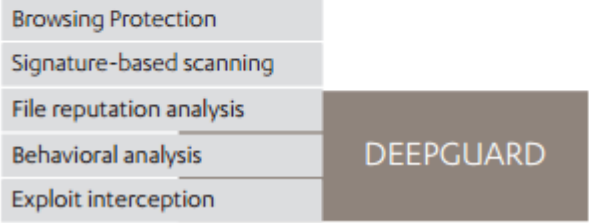
Avast's products meet the recited claim language because it derives security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable.

As shown below, Avast's Endpoint Protection and other antivirus software meet the recited claim language because Avast uses DynaGen technology that includes two back-end classifiers: (1) Malware Similarity Search; and (2) Evo-Gen. See avast! antivirus: security from cloud (2013) at pp. 17; New Toy in the Avast Research Lab (2012) < <http://blog.avast.com/2012/12/03/new-toy-research-lab/> >; Declaring machine war against malicious Android packages (2014) < <http://blog.avast.com/2014/04/02/declaring-machine-war-against-malicious-android-packages/> >.



Malware Similarity Search scans unclassified executable files and creates representations of the files. A representation of a file includes its static properties as well as dynamic "execution traces" discovered by executing the file and logging suspicious operations. Malware Similarity Search scans for over 100 features that are easily identified and relevant to malware classification. Once the representation of the file is generated, the static properties and execution traces of the file are compared for similarity with static properties and execution

	<p>traces of known clean and dirty samples and the file is classified as either clean or dirty.</p> <p>Moreover, if the file is classified as dirty, Evo-Gen creates a generic malware description that includes static properties and execution traces that are shared by the file and other known dirty samples (security profile data including a list of suspicious computer operations that may be attempted by the Downloadable). The goal of Evo-Gen is to produce a brief description that describes as many dirty samples as possible without describing any clean sample. The execution traces in the generic malware description identify suspicious operations that may be attempted by dirty samples from which the description is created, including SEND, WRITE, RECEIVE, DISABLE, ACCESS, MOUNT, UNMOUNT, CALL and LOG operations. By way of example, a generic malware description created for a related group of fake Korean banking Android application packages called Android:Telman is shown below.</p> <table border="1" data-bbox="529 779 1474 915"> <thead> <tr> <th>feature</th> <th>value</th> </tr> </thead> <tbody> <tr> <td>android.permission.RECEIVE_SMS</td> <td>YES</td> </tr> <tr> <td>android.permission.MOUNT_UNMOUNT_FILESYSTEMS</td> <td>YES</td> </tr> <tr> <td>android.permission.CALL_LOG</td> <td>YES</td> </tr> <tr> <td>android.permission.ACCESS_WIFI_STATE</td> <td>NO</td> </tr> </tbody> </table>	feature	value	android.permission.RECEIVE_SMS	YES	android.permission.MOUNT_UNMOUNT_FILESYSTEMS	YES	android.permission.CALL_LOG	YES	android.permission.ACCESS_WIFI_STATE	NO
feature	value										
android.permission.RECEIVE_SMS	YES										
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	YES										
android.permission.CALL_LOG	YES										
android.permission.ACCESS_WIFI_STATE	NO										
<p>1d. storing the Downloadable security profile data in a database.</p>	<p>Avast's products meets the recited claim language because it stores the Downloadable security profile data in a database.</p> <p>As shown below, Avast's Endpoint Protection and other anti-virus software meet the recited claim language because it stores the profile created by the analysis of the downloadable in a database. The information is stored and then used to for future reference.</p> <p>The file's execution traces and any generic malware description created using the execution traces are stored in the avast! Research Lab database for future reference (storing the Downloadable security profile in a database).</p> <p>See avast! antivirus: security from cloud (2013) at pp. 15-18; New Toy in the Avast Research Lab (2012) < http://blog.avast.com/2012/12/03/new-toy-research-lab/ >; Declaring machine war against malicious Android packages (2014) < http://blog.avast.com/2014/04/02/declaring-machine-war-against-malicious-android-packages/ >.</p>										

US 8,677,494	F-Secure
<p>For purposes of this chart, the licensed F-Secure products and services utilizes Real-Time Protection Network (RTPN) and DeepGuard technologies. See https://www.f-secure.com/documents/996508/1030745/deepguard_whitepaper.pdf.</p> <p>As identified and described element by element below, the licensed products specifically listed above meet at least claim 1 of the '494 Patent.</p>	
Claim 1	
<p>1a. A computer based method, comprising the steps of:</p>	<p>F-Secure’s products meet the recited claim language because it receives an incoming downloadable.</p> <p>F-Secure products are software based products that use computer processors for scanning incoming program code, or executable files, data, and other content they receive, performing analysis including sandboxing, creating a profile of the incoming downloadable and sending the information gathered to be stored in a database. F-Secure utilizes a Real-Time Protection Network (“RTPN”), which is a crowd-source means to acquire unknown, potentially malicious files from the Internet and store them on F-Secure’s servers, and process these files thereby creating and propagating protection policies. Unknown files are scanned by F-Secure’s “DeepGuard”. DeepGuard is a heuristic and sandboxed based file scanning service. DeepGuard monitors potentially malicious files, including PDFs. https://www.f-secure.com/documents/996508/1030745/deepguard_whitepaper.pdf</p> <p>2. Multi-layered protection</p> <p>F-Secure’s multi-layered approach to security is comprised of the following modules, each designed to address a particular aspect of the threat landscape and work together to provide a complete solution:</p>  <p>...</p> <p>8. Availability</p> <p>DeepGuard is an integral component of various F-Secure security products, including Anti-Virus, Client Security, Internet Security and Protection Service for Business (PSB).</p> <p>In these products, DeepGuard is activated with default settings, but can also be turned off separately.</p>

https://www.f-secure.com/documents/996508/1030745/deepguard_whitepaper.pdf

PROTECTION FEATURES FOR PHYSICAL AND VIRTUAL SERVERS

Use the following table to choose the features for F-Secure E-mail and Server Security installation package that you can deploy on physical and virtual servers.

Product feature / setting	Physical server (Exchange)	Virtual server (Exchange)
Offload scanning agent	✗	ⓘ
Real-time malware scanning	✓	✓
DeepGuard (behavior based protection)	✓	✓
Use RTPN to improve DeepGuard detection	✓	✓
DeepGuard advanced process monitoring	ⓘ	ⓘ
DeepGuard exploit protection	ⓘ	ⓘ

https://www.f-secure.com/documents/10192/137594/FSC_SVCE_functionality-description_htc_web/98f0fbfb-a8ec-4d75-b042-d20312553aa3

1b. receiving an incoming downloadable

F-Secure’s products meet the recited claim language because they receive incoming downloadables.

As shown below, F-Secure’s products meet the recited claim language because they receive incoming downloadables like PDFs. https://www.f-secure.com/documents/996508/1030745/deepguard_whitepaper.pdf

5.2 Monitoring for document exploits

Some document types, such as Microsoft Word or Adobe PDF, are commonly used to deliver exploits. Thus, any software used to open these types of documents is also subject to greater attention by the second exploit interception method, which scrutinizes these programs closely for suspicious behavior caused by malicious document files.

https://www.f-secure.com/documents/996508/1030745/deepguard_whitepaper.pdf

1c. deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and

F-Secure’s products meet the recited claim language because it derives security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable.

As shown below, F-Secure’s products meet the recited claim language because F-Secure uses DeepGuard looks for suspicious computer operations. (“ DeepGuard does not red-flag a program on the basis of a single action but instead watches for multiple suspicious operations.”)

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.