DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

F-Secure – Infringement of the '154 Patent

8,141,154 - Claim 1	F-Secure Client Security Browsing Protection and DeepGuard
A system for protecting a computer from dynamically generated malicious content, comprising:	F-Secure markets Client Security software. Within this software is a function called Browsing Protection. Browsing Protection is an on the cloud service which runs a plurality of websites through "DeepGuard" which is a cloud-based scanning program. Browsing Protection applies safety warnings to various links across the web which reflects the results of the DeepGuard scan. One of the functions of DeepGuard is to monitor frequently exploited programs while these programs run. Monitoring programs while they run allows DeepGuard to observe and intercept (protecting a computer) malicious code which is not generated until the program is in operation (dynamically generated malicious content). 2. During application execution Even after a program has successfully passed pre-launch analysis and is executed, DeepGuard continues to monitor its behavior as a precaution against delayed malicious routines, a common tactic used by malware to circumvent runtime checks. This form of quiet vigilance also allows DeepGuard to provide constant protection for the user without visibly intruding on their experience by displaying excessive prompts.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

2.1 Process monitoring

Applications are monitored for a number of suspicious actions, including (but not limited to):

- Modifying the Windows registry
- Editing files in certain critical system directories
- Injecting code in another process's space
- Attempting to hide processes or replicate themselves

As legitimate programs will also perform such actions from time to time, DeepGuard does not red-flag a program on the basis of a single action but instead watches for multiple suspicious operations. Once a critical threshold of suspect actions is reached, DeepGuard will block the process from continuing.

If available, file reputation and prevalence rating information from the Security Cloud is taken into account to determine this critical threshold. For example, DeepGuard treats files with a low-prevalence rating more aggressively by lowering the critical threshold of suspicious actions that can be performed before the file is blocked.

EXPLOIT INTERCEPTION

Starting in 2013, DeepGuard also employs two exploit interception methods that extend the dynamic protection of on-host behavioral analysis by focusing specifically on monitoring the processes of programs that are commonly targeted for exploitation and on document file types commonly used to deliver exploits.

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

a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and	F-Secure's cloud-based detection operates virtual environments or sandboxes which run executable code. The sandbox runs files such as JavaScript associated with webpages. At runtime, JavaScript in HTML and PDFs will have a JavaScript function and write malicious code of payload, which will only exist at the time the JavaScript function is called. F-Secure's DeepGuard is configured to detect this behavior, such as injecting code into another processes space. 2. During application execution Even after a program has successfully passed pre-launch analysis and is executed, DeepGuard continues to monitor its behavior as a precaution against delayed malicious routines, a common tactic used by malware to circumvent runtime checks. This form of quiet vigilance also allows DeepGuard to provide constant protection for the user without visibly intruding on their experience by displaying excessive prompts.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

	2.1 Process monitoring Applications are monitored for a number of suspicious actions, including (but not limited to): • Modifying the Windows registry • Editing files in certain critical system directories • Injecting code in another process's space • Attempting to hide processes or replicate themselves As legitimate programs will also perform such actions from time to time, DeepGuard does not red-flag a program on the basis of a single action but instead watches for multiple suspicious operations. Once a critical threshold of suspect actions is reached, DeepGuard will block the process from continuing. If available, file reputation and prevalence rating information from the Security Cloud is taken into account to determine this critical threshold. For example, DeepGuard treats files with a low-prevalence rating more aggressively by lowering the critical threshold of suspicious actions that can be performed before the file is blocked. EXPLOIT INTERCEPTION Starting in 2013, DeepGuard also employs two exploit interception methods that extend the dynamic protection of on-host behavioral analysis by focusing specifically on monitoring the processes of programs that are commonly targeted for exploitation and on document file types commonly used to deliver exploits. https://www.f-secure.com/documents/996508/1030745/deepguard_whitepaper.pdf

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

(ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe;	JavaScript which dynamically generate code is not always malicious. Sometimes, this code is harmless, and harmless, legitimate code (input) can resume running with newly generated code. However, if the sandbox in the F-Secure Security Cloud (security computer) deems the content harmless, it will allow a client computer to run the content (only if a security computer indicates that such invocation is safe). **5.2.1 DeepGuard blocks a harmful application** DeepGuard notifies you when it detects and blocks a harmful application. When the notification opens: Click Details to view more information about the application. The details show you: • the location of the application, • the reputation of the application in Security Cloud, • how common the application is, and • the name of the detected malware. You can submit a sample of the application for analysis. https://www.f-secure.com/documents/10192/1052471/F-Secure_Internet_Security_2014_manual_v.2_en.pdf
a transmitter for transmitting the input to the security computer for inspection, when the first function is invoked; and	DeepGuard is used when a client attempts to access malicious content over the Internet. The client computer sends over the network the JavaScript data accessed to an F-Secure cloud server to be scanned. If the scan reveals dynamically generated malicious code in the JavaScript, then DeepGaurd provides and alert:

DOCKET ALARM

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.