F-Secure DeepGuard™ 2.0

WHITE PAPER
SEPTEMBER 2008

1 Executive Summary

Today's Internet threat landscape is dominated by criminals. A few years ago, they were only just beginning to adopt the use of malicious software (malware). Since then, we have seen extraordinary growth in "crimeware" and other malware for profit. Criminal computer networks have rapidly developed and are entrenched upon the Internet. The enemy now possesses advanced expertise and controls massive numbers of infected computers. The threat faced by consumers is growing and it is ever more complex and sinister.

We at F-Secure actively search for emerging threats. Of those potential new threats, the ones that are the most important for us to define as actual threats are the ones faced by our customers. We developed **F-Secure DeepGuard™ 2.0** technology with this in mind.

Antivirus protection has always been something of a community effort. Within the security industry, we have many close partnerships. We also share sample collections with competitor security vendors for the benefit of all. Outside of the security industry resides ***the most important part of our community, our customers***. When one of our customers submits a potential threat to us, we and our systems take action immediately.

With the introduction of **F-Secure DeepGuard 2.0** our customers will become part of the F-Secure ***Real-time Protection Network***. This will greatly enhance the role of our customer community. All customers with this technology will be active members of the Real-time Protection Network rather than a passive recipient of our services. When a customer encounters a potential new threat, we will be notified instantly. Our customer's voices will be stronger than ever before, without any additional effort on their part. It's all part of the ***Network Lookup*** technology built into **F-Secure DeepGuard 2.0**.

F-Secure DeepGuard 2.0 and the F-Secure **Real-time Protection Network** provide the world's fastest reaction times against new threats, using ground-breaking "in-the-cloud" protection techniques. No other antivirus vendor in the world is currently shipping such technology.

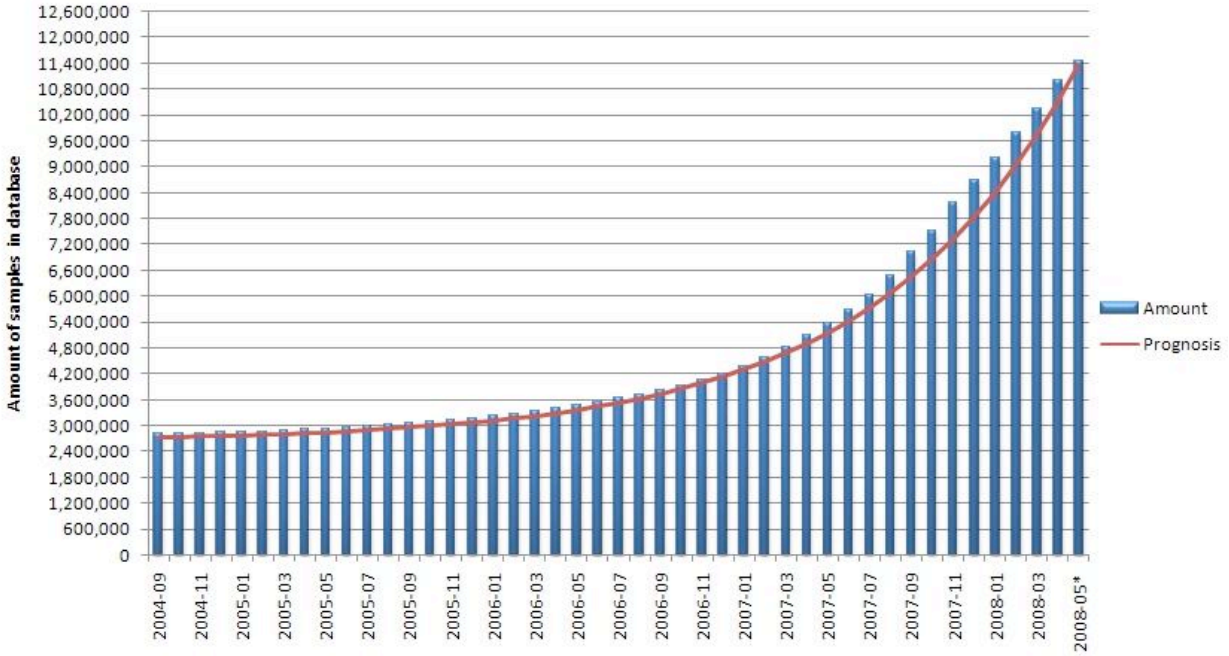
Table of Contents

2 Threat Landscape

The threat landscape of the Internet has changed dramatically over the past several years. Previous year's widespread outbreaks of viruses were developed by teenagers for fame – now they've been replaced by stealthier and much more targeted attacks that are mass produced by professional criminal organizations for monetary gains. This has lead to an enormous increase in the overall amount of malware being distributed to consumers.

The total amount of malware files found during the first half of 2008 was 3 million, some of them with a lifespan of only 30 minutes after which they were automatically replaced with a new variant. The total amount of malware files in existence was over **11.5 million** by the end of May 2008.

With the growing amount of malware and the time it takes to publish signatures, it leaves consumers vulnerable to attacks as they often cannot be detected using traditional methods.

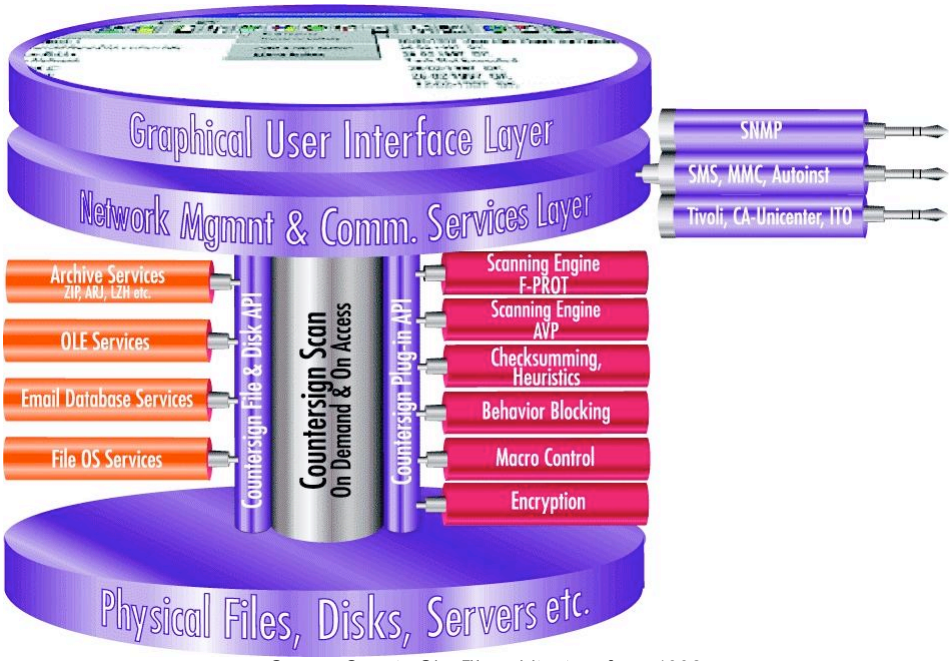


Growth of malware, data from AV-Test.org

3 F-Secure Scanning Architecture

F-Secure has utilized multiple scanning engines in its products since 1998, when **F-Secure CounterSign™** was introduced. CounterSign technology enabled multiple scanning engines to work side-by-side without the issues that usually arise when running two or more antivirus different products.

At that time three scanning engines were used. They all used similar technologies, such as signatures and heuristics to scan for malware. The idea was that the malware that one engine missed, one of the others would block.



F-Secure CounterSign™ architecture from 1998

This logic worked very well for many years. In fact, F-Secure still uses multiple scanning engines even though most the original engines have since been replaced. New engines were needed to protect against new type of threats, e.g. **F-Secure BlackLight** for the detection and removal of rootkits. So while CounterSign itself and the old plug-ins are not used anymore, the same logic is still used in our current products.

4 The Road to DeepGuard

In 2003, F-Secure's Security Labs determined that a new trend was emerging, where viruses and malware weren't just spreading for arbitrary reasons, but were instead being used to create robot networks (botnets) of infected computers. This enabled the people behind the malware to remotely control the computers and instruct them to perform actions such as sending spam or attacking websites. Botnets hid the source of attack and outsourced the financial costs of the computing power used. This enabled malware authors to make money as physically locating them became more difficult and their overhead costs became extremely low.

It didn't take long for malware authors to start using "packers" to obfuscate their malicious code on a regular and often automated basis. This provided them with an easy way to circumvent simple signature-based detections by antivirus products without actually changing anything in the malware code itself. It quickly became obvious that newer technologies were needed to protect consumers.

This was the reason why F-Secure developed DeepGuard, a behavioral based detection engine designed to block new malware from infecting a system by analyzing how the file **behaves** rather than what it **looks like.**

4.1 ***F-Secure DeepGuard***

The first version of F-Secure DeepGuard was released in September 2007 as part of F-Secure Anti-Virus and F-Secure Internet Security. It works by performing a series of checks on a Windows application when it is executed to see not only what it looks like, but more importantly, how it behaves. DeepGuard's behavioral analysis consists of two main components:

- **Gemini** – a heuristic engine that does static checks on the file. It looks for things that are common amongst malware, such as if the file is packed, if it's unsigned, et cetera.
- **Pegasus** – a virtual environment (SandBox[1]). Pegasus executes the file inside its virtual environment and tracks the action of the file without it ever affecting your normal Windows environment.

DeepGuard takes the output of these two components and calculates the behavioral score. Based on this score, a decision is made:

Score	Action
Green	No action, the file is allowed to execute.
Yellow	A dialogue is displayed to the user detailing the system change. The user has the option to allow or deny the application.
Red	The application is automatically blocked and is not allowed to execute.

The DeepGuard scan occurs upon execution of an application, regardless of how it is executed (the user starts the application; double-clicks on an e-mail attachment that drops and runs a program file; drive-by vulnerability via web browser; et cetera) and the scan is only done once. If the same application is started again, DeepGuard recognizes that it has already been checked and takes the same action as previously.

The benefit of analyzing behavior is that a malware application that has only been slightly modified or packed to avoid detection by signatures will still be blocked by F-Secure DeepGuard as the behavior will still be the same as the original malware.

It's easy for malware authors to modify what the malware looks like. But DeepGuard doesn't care about that; **DeepGuard detects malware based on what it does** and malware still has to do what it has to do.

4.2 *F-Secure DeepGuard 2.0*

The combination of the ever growing inflow of samples and the complexity of new malware families forces us to continuously update DeepGuard, to ensure that it is able to interpret and block previously unseen behavior. This process requires a fairly large set of samples and it often takes a few days to collect a large enough collection to train the engine. In the meantime, we rely on traditional signatures to protect customers, but despite F-Secure being one of the fastest vendors in the world to respond to new threats, the delay between a new malware affecting users to our responding with a signature could still be hours.

This simply will not be good enough to fight future threats. We needed to come up with a way of shortening the amount of time it takes from the moment we locate a new malware threat to the moment our customers are globally protected against it.

In 2008 F-Secure DeepGuard was enhanced with a new feature called ***Network Lookups***. This feature enables us to respond instantly to new threats, as the product takes a signature of the file being executed and queries the F-Secure Real-time Protection Network servers to see if it's a good, bad, or unknown file.

If the file is known to be bad, it will be automatically blocked. If the file is known to be good, it is allowed to execute. If the application file is unknown, our systems instantly begin to collect more information. Additionally, DeepGuard's behavioral analysis can be more aggressive in combination with Network Lookups because ruling out massive amounts of known good applications casts a suspicious light on that which is unknown. This use of whitelisting enhances our ability to define the applications that should be blacklisted.

The F-Secure Real-time Network Protection data centers are distributed worldwide and each data center is clustered. These services are so powerful that it only takes a fraction of a second to query the server for the status of an application. **No other antivirus vendor has such "in-the-cloud" protection technology deployed globally.**

The application file reputation is based on detailed execution analysis, static analysis, and the number of users running the application. If the data weighs towards suspicion, the file is automatically flagged for automated analysis. In cases where a definite classification cannot be made by automation, the file is queued to be manually analyzed by one of the analysts in the F-Secure Security Labs.

When an analyst from the Security Labs confirms a new threat, the confirmation only takes 60 seconds to replicate across our Real-time Protection Network servers. Our customers using DeepGuard 2.0 Network Lookups will already be protected from the threat, even while the analyst continues to work on the sample and adds the detection to our signature databases.

Utilizing "in-the-cloud" technologies to confirm the reputation of an application enables F-Secure to respond to new threats ***in a matter of seconds***.

F-Secure DeepGuard 2.0 is already shipping in several F-Secure workstation products and will eventually be a part of all our Windows workstations products.

There is one caveat to this new technology: it requires an online connection. When using your computer offline however, F-Secure's products will work as they always have, scanning files with static scanning engines and DeepGuard without Network Lookups. As most threats target the computer while online (via e-mail or the web), DeepGuard 2.0 and its Network Lookups is always accessible when needed the most.

4.3 ***How does it actually work?***

All Windows application launches are detected by the F-Secure antivirus filter, regardless of how the application was launched, whether by an individual or by a malicious exploit.

1. The application file is scanned with the traditional signature based engines to see if it contains a known threat. If a known malware is detected the file will be blocked.
2. If scanning does not yield detection, DeepGuard 2.0 takes a snapshot of the file and performs a Network Lookup to the F-Secure Real-time Protection Network data centers. The query checks to see if the file has been identified by the F-Secure Security Labs. If the file is known to be good or bad, the proper action is taken automatically.
3. If the file is unknown to the Real-time Protection Network, DeepGuard 2.0 checks the file using its Gemini and Pegasus engines. The file is executed in the sandbox (virtual environment) and the behavior of the application is examined to determine if it should be allowed to run. Combined with Network Lookups, DeepGuard 2.0 has the advantage of knowing that the application is not a known good file. Unknown applications can therefore be treated with more suspicion. DeepGuard 2.0 can consequently be more aggressive with its behavioral analysis.

DeepGuard 2.0 with the F-Secure Real-time Protection Network transmits data up and down "into the cloud". The cumulative effect of this information collection is faster identification of threats being faced by our customers and an easier user experience.

4.4 ***Benefits***

1. Less noise. Without Network Lookups, DeepGuard must interact with the user for Yellow scored applications. Only a limited number of Green applications can be whitelisted and the score of Red applications must be conservative to avoid "false positives". With Network Lookups, large numbers of applications that would have scored Yellow query as good applications. The end result is much fewer prompts to the user. Applications that are determined to be good via Network Lookups also bypass any additional behavioral analysis.
2. More aggressive behavioral analysis. The ultimate goal of the F-Secure Real-time Protection Network is to identify as many known good applications as possible. Elimination of the good from behavioral analysis means that unknown applications can by default be treated with more suspicion. The threshold between Yellow and Red scores can be adjusted and more malicious applications will be automatically blocked by DeepGuard 2.0 as a result, without an increase in the number of false positives.
3. Faster response times. DeepGuard 2.0 Network Lookups provides the F-Secure Security Labs with very valuable information. When our automated systems analyze incoming threat samples, the Lab will now know the number of customers facing the threat. The greater the number of customers, the more critical the analysis. Critical customer cases always come first and now we have a Real-time Protection Network providing us with information. Our customers actively contribute without needing to do anything on their end.

5 In the Cloud Thinking

Each new generation of technology introduced into F-Secure products expands the scope of our analysis. Our layered approach to security makes a great leap forward with the addition of DeepGuard 2.0 and Network Lookups to our Real-time Protection Network.

5.1 Is it a THREAT?

Many years ago antivirus signature scanning engines answered a very simple question. Is this application about to be run on my computer a threat?

Customers submitted samples and we responded with analysis.

The task was straightforward – analyze incoming samples and add the dangers to our detection databases.

5.2 Should it be TRUSTED?

With the introduction of malware-for-profit, everything accelerated. The F-Secure Security Labs developed its infrastructure in order to maintain our response times, but something else was needed to compliment our reactive technologies.

DeepGuard proactive technology was developed and its behavioral analysis asked an additional question. Does this application behave in a trustworthy way and therefore, should it be trusted?

Applications that behave in an untrustworthy fashion can be treated as a threat. So asking "can it be trusted?" provides an answer to our first question. The unknown that appears to be untrustworthy should be treated as a threat.

5.3 Is it KNOWN?

Malware-for-profit is firmly established and further expansion of scope is required. We are no longer simply concerned with threats; we now want to know all we can about every application encountered by our customers.

DeepGuard 2.0 seeks to add to our reactive and proactive technologies by asking if the application is known and what is its reputation.

There is **No Limitation** to the number of known applications that can be identified via Network Lookups. Instead of just critical applications, ALL applications can be identified.

If it is not known, we can treat it with suspicion, which means that any untrustworthy behavior should be considered as a threat and the customer is protected.

5.4 ***Our Customers Benefit***

So the questions continue to expand and the answer to each question helps answer the previous one before it. "Is it known?" helps us to determine trust. "Should it be trusted?" helps us to determine if it should be treated as a threat. Threats should be blocked. Each new layer of our technology makes the picture clearer and our customers safer.

6 Innovation is Key to Success

For us, innovation is key to success and yet again F-Secure is the first company to bring a new technology to the market with the Network Lookups component of F-Secure DeepGuard 2.0.

Previous industry-firsts include the F-Secure BlackLight rootkit scanner, the world's first real-time antivirus on Windows, and the first antivirus to be centrally managed in corporate networks.

About F-Secure Corporation

F-Secure Corporation protects individuals and businesses against computer viruses and other threats coming through the Internet or mobile networks. Our award-winning solutions include antivirus, desktop firewall with intrusion prevention and network encryption. Our key strength is the speed of response to new threats. For businesses our solutions feature centralized management. Founded in 1988, F-Secure has been listed on the Helsinki Exchanges since 1999. We have our headquarters in Helsinki, Finland, and offices in USA, France, Germany, Sweden, the United Kingdom and Japan. F-Secure is supported by a global ecosystem of value added resellers and distributors in over 50 countries. F-Secure protection is also available through major Internet Service Providers, such as Deutsche Telekom and France Telecom.

Europe	***USA***
F-Secure Corporation PL 24 FIN-00181 Helsinki, Finland Tel +358 9 2520 0700 Fax +358 9 2520 5001 http://www.f-secure.com/	***F-Secure Inc.*** F-Secure Inc. 100 Century Center Court, Suite 700 San Jose, CA 95112, USA Tel. (408) 938 6700 Fax (408) 938 6701

We are continually evaluating and developing our products. Please visit www.f-secure.com for the most recent information.

1 Norman SandBox copyright by Norman