



***F-Secure DeepGuard™  
– A proactive response  
to the evolving threat  
scenario***

# ***Executive Summary***

In today's fast-moving Internet-driven world, new opportunities are emerging to take advantage of the latest technologies and increasingly fast connectivity. All of this has enabled people to do more in less time. Unfortunately, this trend of empowerment is not only available for the good, but also for various questionable and criminal activities. This has led to a constant and pressing need for faster and more intelligent technologies to protect the unwary.

Providing efficient proactive protection against malware has long been one of the major goals in developing antivirus software. The updates required for traditional reactive fingerprint-scanning to work have always been problematic. Initially because of rudimentary data networks causing scattered distribution of new fingerprints. In recent years increasingly fast-spreading malware outbreaks have made it difficult to ensure all end users have the latest protection in place. Attempts to solve these problems have been made since the beginning. Heuristic scanning techniques and rudimentary behavior blockers have been implemented in many antivirus products for over a decade. The problem so far has been that these proactive technologies tend to create a lot of false alerts due to their inability to accurately predict program behavior.

The introduction of the F-Secure DeepGuard technology is, however, a milestone that sets new standards for proactive protection technologies. F-Secure DeepGuard's approach is holistic and ties together many core technologies used for the protection of computers. This enables F-Secure DeepGuard to make a smarter and more accurate analysis of the unknown malware it encounters. F-Secure DeepGuard will in most cases be able to accurately detect and block unknown malware without expert help from the user, thanks to the tight cooperation between a wide range of sensors and protection modules. It combines sandboxing, behavior blocking and advanced heuristics in a unique way. All F-Secure DeepGuard installations world-wide also form a network that works together with the signature-based scanning system to form a strong and lightning fast defense against a new generation of skilled and motivated malware authors.

# Contents

<b>Executive Summary</b> .....	<b><i>i</i></b>
<b>1 Reactive or proactive?</b> .....	<b>1</b>
1.1 Reactive protection – the traditional way .....	1
1.2 Proactive protection – instant intelligent protection.....	2
1.3 The threat scenario – what’s needed out there?.....	3
<b>2 F-Secure DeepGuard in action</b> .....	<b>5</b>
2.1 Technical implementation – Deep visibility is essential .....	5
2.2 User experience – Adapting to user skills.....	5
2.3 F-Secure DeepGuard – A global network.....	6
<b>3 Conclusion</b> .....	<b>7</b>

# ***1 Reactive or proactive?***

## ***1.1 Reactive protection – the traditional way***

Traditional reactive scanning for malware means that suspected malware samples are analyzed by a virus analyst in a lab. The researcher makes a decision about the nature of the sample. Code for detection and removal is added to a definition database, should the sample be classified as malware.

Traditional reactive scanning has been the backbone of most antivirus products from the beginning, and will continue in this role for the foreseeable future. This does not, however, mean that it's a perfect technology. Reactive scanning technology has several shortcomings, but its flexibility, accuracy and adaptability has still not been rivaled by any other available technology.

The key difference with reactive compared to proactive technology is naturally the intelligent human needed to handle malware samples and issue updates. The technology may be reactive, but it ensures at the same time that the antivirus researcher gets the last word. The bad guy makes the first move and the good guys respond. An analogy of this is the action of law enforcement agencies worldwide. Criminals commit crimes and the police investigate. A criminal may get away with a crime once or twice, but as soon as he is in jail, his crime spree ends.

The key issue in reactive protection is of course speed of response. A lack of connectivity reduced the spreading speed of malware during the nineties. This same technical limitation was naturally also an issue for the traditional antivirus updates. But due to the relatively slow propagation of malware, it was still quite easy to keep protection updated within acceptable levels.

The explosive penetration of high-speed broadband connectivity created a much more powerful environment for antivirus definition database distribution in the late nineties and in the new millennium. Unfortunately, it also created a much more fluid environment for malware to spread. The traditional passive computer virus was replaced by the actively spreading worm. Typical times from first observation to large-scale outbreak dropped from months to hours. And with the latest modern threats, such as the so-called targeted zero-day attacks, the time to react is literally coming down to zero. The researcher in the lab and the testing of virus definition updates have become the new bottlenecks.

## ***1.2 Proactive protection – instant intelligent protection***

The drawbacks of reactive protection were already recognized during the early years of virus protection software. The need to constantly monitor the situation and respond to new threats created the need for a specialized organization, the virus research laboratory. The working conditions in a virus laboratory are unique, highly specialized skills are required and the work is done under extreme time pressure. But no matter how skilled and fast the lab team is, there is always a time lag before the reactive protection update can be delivered to the customers. A lot of effort has been put into solving this problem.

Heuristic scanning has been implemented in antivirus scanners almost since the beginning. This was the first attempt to solve the problem of response times and provide instant detection that didn't require updating. Heuristic scanning works by looking for potentially malicious functionality rather than for known malware. The scanner can identify pieces of code that are typical to viruses, and flag the file as suspicious if it detects certain combinations of these attributes. This is a good start, but there are always accompanying problems with this approach. If the scanner is set at sensitive with the aim of detecting most malware, then the number of false alerts will rise. And a false alert may cause as much headache as a real infection. This makes heuristic scanning a feasible tool for the expert user, but the potential of false alerts limits its usefulness for non-technical users.

Behavior blocking and HIPS (Host-based Intrusion Prevention System) are becoming typical components in more modern proactive protection systems. These systems do not only examine code in files like the traditional heuristic scanners used to do. These systems implement sensors in the system that intercept actions performed by running programs, and are able to block the actions if needed. These systems get a much more accurate picture of what the running program is up to as they are able to monitor and control its actual runtime actions. But the basic problem in proactive protection still remains. The executable itself is not identified and the systems must make a decision about its nature based on the actions it performs. The algorithms involved can be tuned to catch everything – and produce a lot of false alerts. Or it can be tuned to not bother the non-technical user, potentially letting malicious code to be executed. In essence, heuristics is a tradeoff between detection accuracy and the frequency of needless interruptions to the user – something often called the “noise level” of the solution.

There is also another problem with proactive protection. The purpose of proactive protection is to add protection that works even without anti-virus updates. This often makes the solution more static and easier for malware authors to analyze overall. The malware author can modify and fine-tune their code and test it against the proactive system. A skilled malware programmer will be able to figure out what kind of patterns the proactive system is looking for, and alter the malware so that it doesn't trigger an alert. Proactive protection basically means that the antivirus software is making the first move

and lets the malware author respond. Proactive protection systems can naturally be updated and tuned remotely by the antivirus lab to deal with any new scenario. But that puts us back into the reactive model with its attendant problems.

Looking at the pros and cons of the reactive and proactive protection approaches, it is easy to understand that an ideal solution should probably include elements from both of these worlds. And ideally, both technologies should be working seamlessly together, complementing each other to form a truly solid overall solution.

### ***1.3 The threat scenario – what's needed out there?***

The evolution of data communications used to be the main factor that controlled the global malware situation. The ability to exploit a new communication channel and use it for malware replication was typically the key trigger for a new and more powerful generation of malware. The situation has, however, changed dramatically in the 21<sup>st</sup> century. Broadband connectivity is widespread and high-speed data communication channels are no longer the bottleneck for malware. The new key to success for malware has become its ability to accurately locate targets considered useful for the malware author. This is related to the dramatic shift in the drivers and motivation factors for malware authors. Malware is no longer written as an intellectual challenge. Nor is today's typical malware author a clueless teenager who is attracted to the mystique of malware-coding. The new driver for malware authors is quite simply money.

The Internet is no longer a playground for computer enthusiasts. Nor is it a pure marketing channel or a place to just show a company's online catalog. The Internet has become the world's fastest growing marketplace and more and more of the contents on the net is related to eCommerce in one way or another. This development has given birth to a new generation of malware authors – the cyber criminals. They are far more motivated than their clueless teenage counterparts. They also have better possibilities to maintain the skills necessary to develop high-quality malware code. And last but not least, their ideal malware look very different from the teenager's creation because their goals are different.

The objective of malware written by a cyber criminal is typically to steal bandwidth, computing capacity or information. The attack may be carefully targeted to one destination or aimed at suitable computers around the world. But the number of infected computers is typically limited in both cases. The clueless teenager thinks it is cool when his creation causes a massive outbreak and headlines all over the world. The same scenario is a failure for the cyber criminal. The attention raises computer users' awareness and makes them clean up infected computers and install the appropriate protection solutions. The ideal scenario for the criminal is to create a larger number of smaller outbreaks that more carefully target selected victims. This makes it possible to break into the same number of relevant targets, at the same time flying under the media's radar without attracting attention. This will

naturally require more development work for the malware author. But this is not a problem as the profit from the criminal activity in most cases well outweighs the effort.

The challenge for antivirus vendors lies in the fact that analyzing a new virus requires the same amount of work in the lab regardless of how large the outbreak is. A scenario with ten smaller outbreaks is much harder to handle than one big one, even if the total number of affected computers may be roughly the same. The sample submissions to the lab may also be slower in case of smaller outbreaks. It takes longer for a sample to hit a honey-pot computer on the Net. Effective proactive protection could theoretically deal with all ten outbreaks and block them. But the new generation of malware authors is not only able to produce more code. They are also able to produce better code, and especially code that has been tested against existing proactive systems.

The conclusion is that the malware authors' ability to produce more code makes traditional reactive scanning less effective. And their ability to produce better code limits the usefulness of proactive protection. This naturally means that a successful protection system must be able to combine the strong aspects of both techniques to be successful in the fight against the new generation of malware authors.

## **2 F-Secure DeepGuard in action**

### **2.1 Technical implementation – Deep visibility is essential**

F-Secure DeepGuard is by nature a sandbox, a behavior blocker and a part of the security lab's research methods and tools. Deep, under-the-surface visibility into what a given software is doing is essential in all three roles.

F-Secure DeepGuard achieves this needed visibility mainly by using two different technologies, sandboxing and triggers that monitor system activity. The sandbox creates a virtual environment where suspicious software can be run without risk of compromising system integrity. Most malware programs will initiate actions that reveal their true nature when run in the simulated sandbox environment. These actions can't harm the computer system because they are performed inside a simulated environment before the malware is actually executed by the operating system.

A sandbox alone can't, however, catch all behavior that can be termed malicious. Sandboxing is quite time-consuming and the simulation is not perfect. This is where the system triggers take over. A wide range of carefully selected system activities are monitored by F-Secure DeepGuard and actions performed by a certain process form a sort of a fingerprint. This pattern, together with information from the sandbox analysis, can be used to constantly monitor the behavior of processes that have passed the initial screening by the sandbox. Any new action that may be significant is added to the overall picture of the analyzed software and F-Secure DeepGuard can at any point alter the classification of the software and take the necessary actions to ensure system integrity.

### **2.2 User experience – Adapting to user skills**

The data collected by the sandbox and the system triggers are used by a local artificial intelligence system. This system is one of the key factors that make F-Secure DeepGuard unique. Simple HIPS-systems typically intercept suspicious system activities and lets the user decide what to do with the offending application. This approach may be fine for expert users with the skills to interpret the information and make the right decision. Non-technical users are, however, confused by systems of this kind and are likely to put their computers in jeopardy by unintentionally giving the wrong answer to technical questions that they have no possibility to understand.

F-Secure DeepGuard has been designed with this in mind. There are three different operation modes that are developed for different types of users. The expert user can still have control over the system and approve blocking actions proposed by F-Secure DeepGuard. But most users will probably run the system in Normal or Automatic mode. Both modes minimize the number of questions to the user. The Normal mode may ask the user's permission if the

case is unclear and blocking the actions could lead to breaking legitimate software. The Automatic mode never asks the user any questions.

The key to success for the Normal and Automatic modes lies in the artificial intelligence system that is able to determine whether an application's overall aim is to do something malicious or not. F-Secure DeepGuard is able to provide extremely reliable detection because of its unique multi-tier approach. The sandboxing provides a good base profile for the executable that is about to start and enables early blocking of many malicious programs. The system triggers that take over after program launch update the program profile and enable the artificial intelligence to build a clearer and clearer picture of the programs attempts when it is running. This means that the program isn't judged based solely on single operations, but rather by the overall picture of what it has done so far, what it is doing right now and what it is likely to be doing next. In this regard, F-Secure DeepGuard is a lot like a virtual virus research lab inside the computer.

### **2.3 F-Secure DeepGuard – A global network**

Traditional antivirus technology has typically been system-centric. The scanner examines one system at a time without any knowledge of what goes on in the world around it. Fast spreading worms may exploit this and attempt to infect large number of computers before they get updated virus signatures.

F-Secure DeepGuard is a departure from this way of thinking. Installations around the world are constantly examining a large number of unknown, possibly malicious applications. Using knowledge from all these installations provides a huge benefit to the researchers in the lab.<sup>1</sup> It makes it possible to detect and investigate possible malicious programs a lot faster than before. It provides both early samples of new malware and global statistics that help the researcher evaluate how rapidly the malware is spreading.

All this leads to faster and more accurate detection of the new threat. It is enough that a handful of F-Secure DeepGuard installations detect vague signs of malicious activity, all other installations world-wide will soon benefit from this and have accurate and up-to-date information about the new threat.

---

<sup>1</sup> Any information collection for this purpose is done according to legislation and good privacy protection practices. When F-Secure DeepGuard finds malicious software, the user is prompted to submit sample information to F-Secure virus research lab. The user can also deny this sample transmission.

### **3 Conclusion**

The global cyber threat scenario is becoming more and more challenging for antivirus vendors. The main reason for this is the new generation of cyber criminals who have become the dominant malware authors. A large number of smaller malware outbreaks suit their needs better than large worldwide pandemics. This tactic enables them to fly under the radar and avoid unnecessary media attention. The rapid development and large number of unique new malware keeps the antivirus labs at least as busy as during the era of massive global outbreaks. The challenge to keep pace and maintain a sufficient reactive protection system is getting tougher, despite the fact that the virus problem may seem to be declining based on media coverage.

The increased skills of the cyber criminals are making existing proactive protection techniques less effective. Simple proactive protection is by nature static and the new generation of malware authors have the skills and resources to test their code against the major antivirus brands' proactive scanners. Reactive scanning uses human intelligence in the research lab to fight malware, but the cure always comes with a delay. The increased skills and resources of the cyber criminals make it possible for them to fight both technologies with a fair amount of success.

The most effective defense in this situation is to couple reactive scanning and proactive protection tightly together. F-Secure DeepGuard forms a global network that, in addition to proactive protection, provides increased visibility about new threats for the researchers in the antivirus lab. The instant analysis of suspicious software provides a global sensor system that gives the researcher a chance to react to vague indications of malware that no artificial intelligence could flag as malicious with sufficient certainty. In other words, all F-Secure DeepGuard installations are coupled to both the local artificial intelligence in the same computer and to a researcher in the lab with human intelligence. This enables F-Secure DeepGuard to combine the strengths of both reactive scanning and proactive protection, dramatically reducing the overall reaction time to new threats while at the same time maintaining the highest level of detection accuracy.

## 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.

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

*"F-Secure" and the triangle symbol are registered trademarks of F-Secure Corporation and F-Secure product names and symbols/logos are either trademarks or registered trademarks of F-Secure Corporation. All other product and company names referenced herein are trademarks or registered trademarks of their respective companies. F-Secure Corporation disclaims proprietary interest in the marks and names of others. Although F-Secure Corporation makes every effort to ensure that this information is accurate, F-Secure Corporation will not be liable for any errors or omission of facts contained herein. F-Secure Corporation reserves the right to modify specifications cited in this document without prior notice.*

*No part of this document may be reproduced in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of F-Secure Corporation.*

*We are continually evaluating and developing our products. Please visit [www.f-secure.com](http://www.f-secure.com) for the most recent information.*