AV-LAB

THE INDEPENDENT ANTIVIRUS TESTS

Antivirus for your company

Why not Emsisoft?

December 2016

Do you work as an IT administrator? Do requirements imposed by decision makers in your company regarding cyber security suggest, that probably you don't need a complex antivirus software with integrated monitoring and management functionality? Maybe your actions focus only on a solid antivirus protection (that won't slow down workstations, which aren't the newest ones anymore) and in addition you have experienced the hard way, that popular antivirus applications in your country are already a bit overrated? If your answer for at least one of the questions above is affirmative, it's a right time to finally try something different — a solution, which will do its task — a task for which it was created. Nothing more.

Why not Emsisoft?

Nowadays, there are plenty of security applications for businesses. Offers of individual developers are really interesting — in most cases they meet the requirements of small and medium-sized businesses in our country, and selection of a particular solution isn't an easy task.

However, modern "antiviruses" have a fundamental flaw — or offer a solid protection against a full spectrum of malware (at the same time don't have practical monitoring and management functions, beneficial from the point of view of a particular company), or just the opposite — administrators are so accustomed to a desired function (e.g. remote desktop integrated with antivirus software), that are willing to sacrifice some security mechanisms to make their job easier.

> *How about Axence nVision Pro solution correlated with an antivirus software? It's pretty good combination, because we receive a comprehensive solution for employees activity monitoring and company assets protection.*

Crypto-ransomware, threat of 2016

Unique statistics, presented in the protection test against crypto-ransomware, didn't come out too well for companies in our country. The results verify how ransomware threats have developed over the last few years and what this phenomenon has caused. Our analyzes show, that protection against this type of constantly evolving threats just isn't the best in most antivirus applications, and repeating like a mantra the same "best practices" of using a computer (don't click on attachments, don't open suspicious websites, etc.) fails to fulfill its expectations or simply doesn't reach people who could benefit the most from.

Our latest test has proved, that the more well-known antivirus solutions protection against files encryption is effective — in this matter obviously we could use a different methodology (by configuring individually every security suite and enabling their maximum protection), but in comparative tests settings other than the default are not fair, unless it was clearly included in the methodology.

Our test results stand as they are, although not all developers are happy about them (let us keep details of those conversations private), we have to mention some of the comments: several developers disagreed with our test results to such an extent that they wanted us to test

only “proven” samples — we can here argue, what does “proven” mean or proven by whom. Unlike the AV-Comparatives, we strongly disassociate ourselves from using samples provided by the developer, and we don’t agree when anyone is suggesting what kind of research material we should obtain and from who.

> *If you want to find out how modern antivirus software for businesses and home users deal with the latest crypto-ransomware threats, we recommend to read our latest test, which exposed the weaknesses of some products in terms of inadequately selected default settings.*

In the 21st century, there are no companies without access to the Internet

This is a very risky statement, but we want to bring up two points. The first concerns running a company in the 21st century and safeguarding assets. The second concerns our opposition to the words of an expert working for Google — Darren Bilby, who stated that “antivirus tools are a useless box-ticking exercise”.

1. How to conduct effective business activities without an access to the Internet? Every company could ask this question, if the Internet crashed all over the earth. Impossible? This happened in October, when unidentified perpetrators carried out a successful attack on Dyn — DNS service provider, without which user communication with websites may be much more difficult. During this attack, platforms and services like: Netflix, Twitter, Spotify, Reddit, CNN, PayPal, Pinterest and Fox News, as well as The Guardian, New York Times and Wall Street Journal for a few hours have encountered significant issues in running their businesses, which are based on the Internet.

Probably there is no longer such an economic activity, which in developed or developing countries doesn’t benefit from advertising (social media), instant contact with counterparties and immediate access to global information. Thus considering the statement above, we can argue that every Internet user actually needs protection against different types of attacks or at least control, monitoring and privileged access to specific resources in the cloud, network or Intranet.

2. At the KIWCON conference about security matters, Darren Bilby stated that while antivirus software are useful tools, their domination should end. Is that so?

AVLab, web portal about network security probably “shouldn’t saw off the branch it is sitting on”? — Someone might accuse us of an unilateral approach to the problem. But considering the multifaceted statement of “antivirus software usefulness”, Darren words appear to be poorly thought out.

Darren, a security expert, understands contemporary threats and antivirus applications weaknesses, but can his company — Google — live without antivirus software? We would like to see it.

Let’s split this statement into several components:

a. Security experts don't always take into account additional factors, that favor the use of antivirus applications.
b. Individual users can live without antivirus applications, as long as their knowledge regarding cyber security is on an intermediate level.

c. Private companies and public institutions mostly employ ordinary people, who aren't trained on how to recognize attacks. If you put yourself in the place of such company owner — employing 100 people, would you put at risk your information security (which translates into a financial liquidity), and completely abandon the antivirus software?

Emsisoft for businesses

Emsisoft products among competitors are situated... it depends which solution they will be compared to. Emsisoft Anti-Malware, antivirus for workstations (by the way, it's technological copy of Emsisoft Anti-Malware for individual users) is simply good. Although the on-premise Emsisoft Enterprise Console doesn't support mobile devices, remote desktop, cloud and system updates management, it can provide a treat for companies, that know what they need — and don't demand from antivirus application all the mechanisms, which give practical form to a monitoring and management policy.

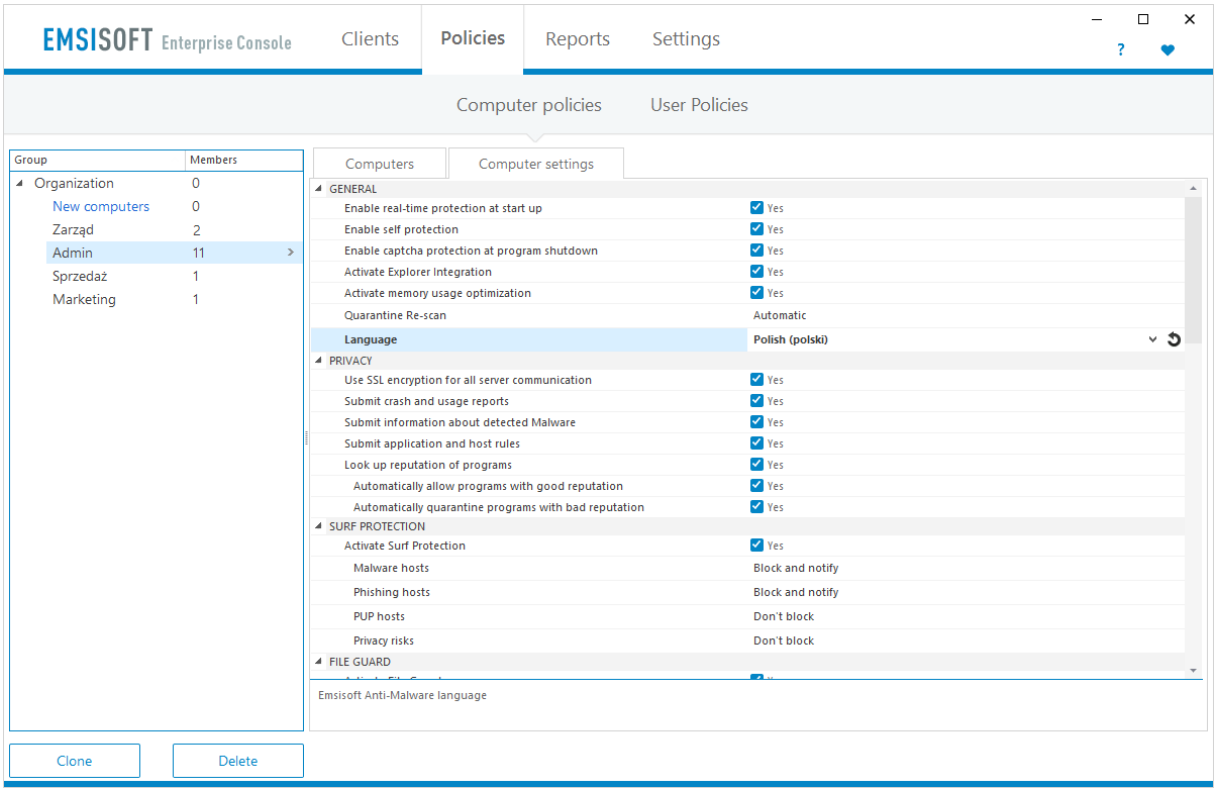

Figure 1 Every IT specialist will find himself comfortable with on-premise *Emsisoft Enterprise Console, even if hasn't used similar products before.*

In practice, implementing protection on workstations doesn't differ from generally accepted standards in this area. IT specialists can do it in several ways:

a. by importing workstations connected to a company domain or workgroup,

b. by searching a local network using the PING protocol — workstation with Emsisoft Enterprise Console installed will check availability of computers inside parent subnet or other local network.

It is worth noticing that console doesn't demand from computing environment having own domain inside Active Directory. It means, that Emsisoft Enterprise Console will work in small businesses.

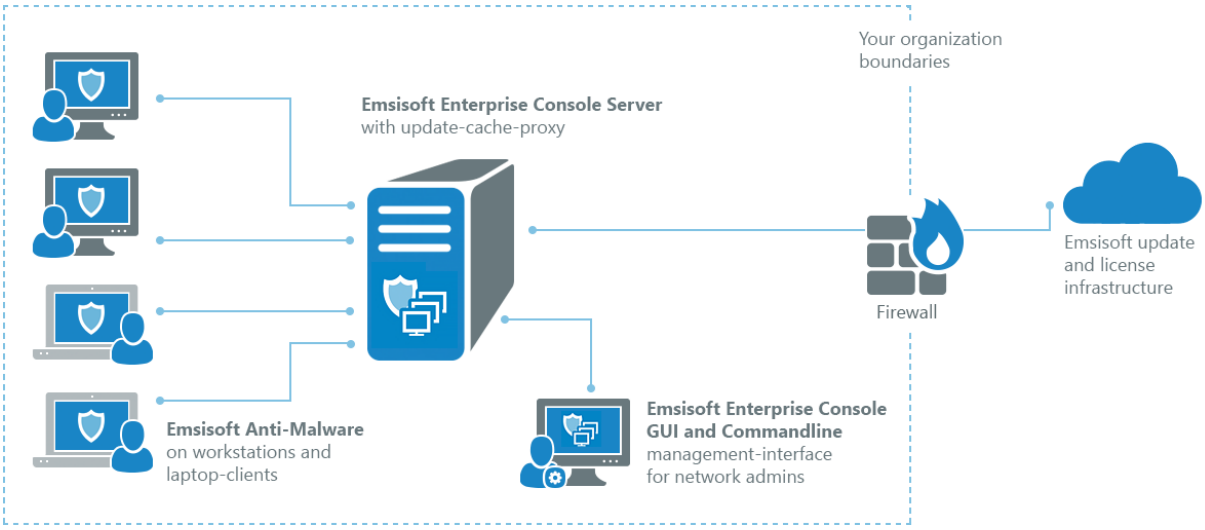

Figure 1 Extended dialogs in the event of installation failure deserves our attention. The console sends detailed error codes, which helps with a problem solving. Unfortunately, not all competitive solutions have such an important feature.

As for the settings that can help administrator with controlling workstations, everything is in place here: it's possible to create exceptions for websites (including traffic capture to an own proxy), define scan schedule, create exceptions for scanned files and folders — it seems that all the basic and mandatory functions are in place. However, we have that impression that something is missing here — although, it's probably caused by too frequent contact with more complex solutions of this kind.

Emsisoft Anti-Malware tests

To verify the effectiveness of real-time protection, we have installed Emsisoft Anti-Malware on the default settings. A signature database has been updated to the latest version, and antivirus has access to the Internet throughout the test period.

Real-time protection

The test was divided into three phases, wherein each subsequent was depended on the previous one.

1. The first phase included blocking malicious software already installed on web browser. 40 malicious websites were run sequentially on each day, which led directly to malicious files, among others: trojans, backdoors, ransomware, downloaders.

2. The second phase was checking the effectiveness of local protection against threats, that haven't been detected in the first phase.

3. The third phase was reflecting the heuristic protection — if the risk hasn't been blocked in the second phase.

Protection test against phishing websites

This test was intended to check detection of phishing websites, which attempt to obtain sensitive information, like bank account and credit card details or login data for various online services. On each day of testing, phishing websites weren't older than 24 hours after the first online release.

Day	1	2	3	4	5	6	7	Total
Real-time protection	40/40 --- 1: 16 2: 10 3: 14	40/40 --- 1: 10 2: 14 3: 16	40/40 --- 1: 12 2: 7 3: 21	40/40 --- 1: 24 2: 10 3: 7	40/40 --- 1: 17 2: 5 3: 18	40/40 --- 1: 11 2: 2 3: 27	40/40 --- 1: 11 2: 14 3: 15	**280/280**
Phishing	38/40	39/40	35/40	32/40	39/40	39/40	37/40	**259/280**

A very good threat blocking mechanism based only on behavioral protection deserves special attention. Obviously, Emsisoft antivirus applications feature two files monitors, but the mechanism that sets these products apart from competition is the Behavior Blocker.

Performance

> *Due to the fact that tested agent for workstations, Emsisoft Anti-Malware is the same application, that is used by individual users, we kindly invite you to read the Emsisoft Anti-Malware 12.0 review and performance test in the dedicated article.*

Conclusion

Does the Emsisoft product for businesses deserve our recommendation?

Disadvantage of the solution is technical support, which is available only in English language (although, official Emsisoft resellers in Poland, companies like Mojosoft, Vebo and e-antywirusy are doing their very best) — it may become an issue impossible to pass through for a certain group of IT specialists in Poland, but most importantly — in tenders, in which interested party requests developer or distributor to verify, if its products meet a demand for the various antivirus software, e.g. support for specific operating systems, protection against ransomware (indicating a particular module), remote desktop feature, creating exception in a manner provided by particular developer, scanning email protocols, protection against spam using Bayesian algorithm or server addresses stored in RBL and technical support in Polish mentioned before.

From many organizations point of view, especially public institutions and state-owned companies, these aspects are an inseparable part of the Terms of Reference document in public procurement. Actually, this problem doesn't exist for private businesses. Among these customers, Emsisoft may find favor with administrators.

https://avlab.pl

For press (big size resolution certificate): https://avlab.pl/dla-prasy

About AVLab

AVLab brings together enthusiasts of antivirus software and web safety. Our activities include program testing and sharing results of our analyzes with all Internet users. We are not controlled and/or linked with any software developer.

AVLab tests are independent and take place in conditions close to reality. Don't be guided by our results when making a final decision in choosing antivirus program. In order to make a final choice we suggest to read tests from other independent laboratories that use different methods and techniques for testing antivirus software. In addition, decisions depends on personal preferences, specified features, efficiency, detection rate, impact on system performance, user interface, price, usability, compatibility, language, technical support quality and many other factors.