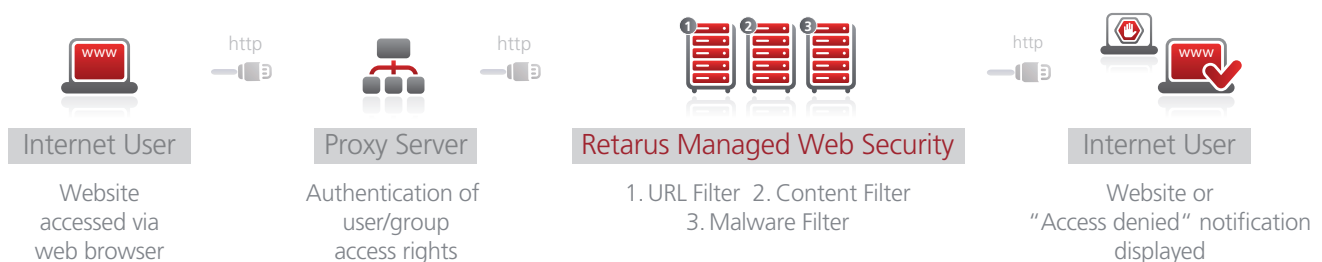


Retarus Managed Web Security

Websites infected by viruses and spyware, excessive private use of the internet by your employees and unwanted content all endanger the security of your company's IT and have a negative effect on productivity. The IT analysts at Gartner recommend web filters to implement rules on use of the internet within the company. Retarus Managed Web Security offers comprehensive protection against threats and unwanted internet content. You specify which content your employees can access and which they cannot. Thus, you implement your policies on internet use consistently, sustainably improving company security. And detailed reporting ensures that internet use by your employees is fully transparent at all times.

How it works



Your benefits

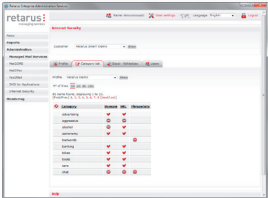
- Efficient protection against spyware, viruses and unwanted internet content
- Consistent implementation of web use policies
- Convenient configuration using categories and lists
- Transparent reporting by domain, website and filter categories
- Synchronization with your directory service



Reliable protection against unwanted content

Filter efficiently – surf safely

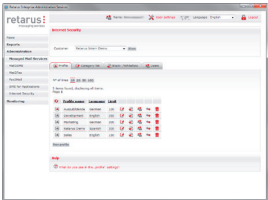
Gartner specifies the following central requirements for a web filter solution: filter options for URLs, a malware recognition function and a reporting function. With Retarus Managed Web Security you have efficient control of web use at your company. Block unwanted web offers like chat, social networks, games or erotic sites using more than 80 filter categories. You ensure the productivity of users and comply with legal requirements – for instance by block-ing youth-endangering contents for minor trainees. Filters are updated daily ensuring constant, efficient protection.



Convenient configuration using categories

Control thanks to flexible configuration

Black and white lists ensure more granular control of web access rights. You can block or release individual websites. So, for example, you can block the use of certain social networks like Facebook while permitting others such as Xing for a selected group of people. Websites that are not included in filter lists or blocking lists can be easily blocked using categorized word lists. Each word on these lists is assigned a defined value. If the sum of all “bad” words on a website accessed exceeds a limit you have set the site will be blocked. On request, we will adjust the lists to your requirements – to ensure maximum control of web content.



Control web access using profiles

Security for your infrastructure

Retarus Managed Web Security provides optimal protection against spyware and viruses. As soon as there is an attempt to access infected websites the Retarus infrastructure recognizes the dangerous content and prevents the site being downloaded. You can also inhibit downloading of specific data types like EXE, LNK, or SCR files. In this way you effectively avoid harmful data reaching workplace computers.

Transparency through detailed reporting

Experts at Gartner advise using solutions which allow comparison with directory services to authenticate users and control access rights. To configure categories and lists for Retarus Managed Web Security you use the web-based administration portal. Here you can also enter users, groups and profiles. Incorporate an in-house proxy to authenticate users. Profiles can be synchronized with your Active Directory or any other directory services. Detailed reports make the use of the internet by your workforce transparent. For example, you will be able to see how often and when individual websites or domains are called up within a specific period of time and the respective filter categories which have been assigned. Incidentally, you can easily extend this protection to mobile employees. Put us to the test, we'll be pleased to help you!