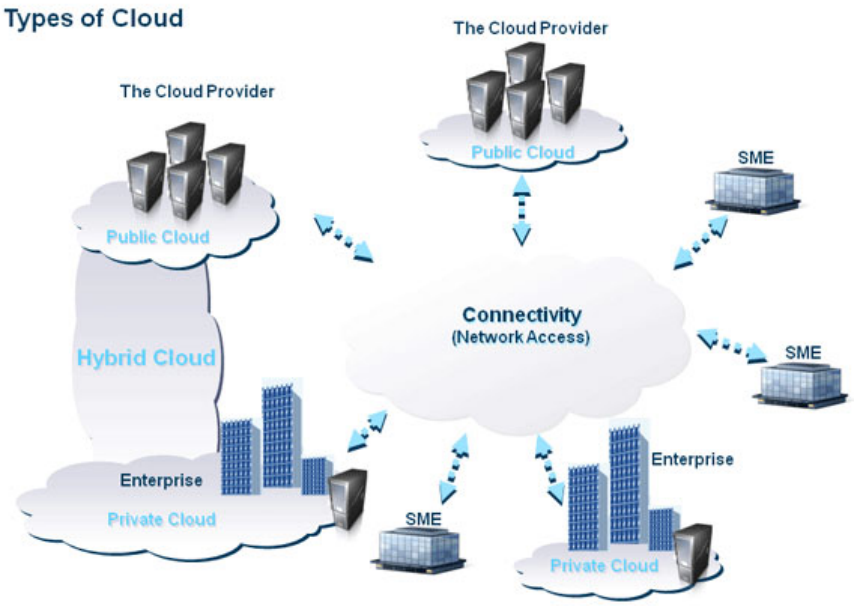
Cloud computing transforms how to prevent viruses?

Many people believe that when cloud computing becomes big, security solutions and anti-virus running on personal computers will soon fall into the 'afternoon market'.

Many people believe that when cloud computing becomes big, security solutions and anti-virus running on personal computers will soon fall into "afternoon market".



Imagine in the future, when individual users and businesses begin to gradually switch to Internet-based applications or also known as cloud services (cloud service), what will happen to the security utility? and anti-virus for personal computers? The question is whether security solutions running on personal computer platforms are now flexible enough, and most importantly, how to change to keep up with the rapid growth of security needs. Confidential on the online platform.

Previously, many security and computing experts had predicted the decline of the security industry for PCs before the "online" wave of services and applications. However, the traditional security solution business model has yet to rush "surrender" because security companies still believe that users will definitely have to use a personal computer at some point - like turning it on and off. The most important, is to start the browser to use cloud computing services.

This prediction comes from the increasing number of business users and universal users moving to internet-based applications, thereby reducing the proportion of anti-virus utilities on personal computers. A study at the University of Michigan (USA) shows that cloud computing services also pose many risks related to viruses in particular and malicious software (malware) in general. There is also an opinion that when data of users and businesses are hosted on cloud computing services, it is considered that the invisible security has been "entrusted" to suppliers. service. However, there is no basis to show that cloud computing is an important driving force for the security industry.

A recent report by *G Data SecurityLabs* shows that the number of computer viruses globally is growing rapidly - only in the first half of 2010 there were 1,017,208 viruses detected, about 50% higher than last year. **G Data also forecasts that the total number of newly discovered viruses will reach a record 2 million by the end of the year.**

Most security firms believe that security threats for personal computers are growing in both quantity and danger, from which they "stimulate" for more powerful multi-layer security services. In parallel with maintaining and constantly updating security and anti-virus utilities running on personal computers, security companies are also more proactive in integrating online components into existing solutions. Friends Instead of completely replacing the security utilities for personal computers, integration with cloud computing will somehow help expand the security utility market in all respects - applications for personal computers and both security services run on cloud computing. It can be said that, up to now, anti-virus utilities running on personal computers still hold a very important position and show market leadership at least within the next 3 to 5 years.

The future of the security industry in the next five years will fundamentally revolve around the following issues:

*** Anti-virus on cloud computing:** Of course, cloud computing cannot "swallow" the security industry in general and antivirus in particular, but they will become an important component of the market. Manufacturers of antivirus applications will deploy cloud-based components in traditional solutions, otherwise they will not be able to compete in several market segments. The benefit of the cloud-based anti-virus system is that the scanning will be done more quickly and comprehensively because the virus is screened through a variety of technical layers, identifiers and service versions.

*** Safe list:** Current security solutions often disable default "unapproved" tasks on a personal computer or local network - such as launching a malicious software or transferring news to the 3rd organization is not allowed. Currently, Bit9, Sophos, McAfee, Symantec and Microsoft all apply this method.

*** "Virus-resistant" computer:** Intel recently acquired security vendor McAfee to be able to create chipsets capable of resisting virus infection. Over the next 5 years, programmed hardware devices, from chipsets, to computers, mobile phones, and network devices, are believed to be stronger.

*** Socializing data about viruses:** Last year, Symantec used a reputation-based layer of evaluation mechanism to assess the security of new software or applications from firms. production, small and no-name developers. The solution of using "crowd intelligence" and "trust" data warehouse from the user community will help Symantec calculate the credibility (safety) or "bad reputation" of an application. Symantec now sees the technology as an important component in its antivirus and security suite. In the future, anti-virus applications will probably follow this "open" model to become more popular to discover newer, more dangerous vulnerabilities.

*** Filtering content on the internet:** Another change for anti-malware and virus prevention is the deployment of web filtering - this can be considered a new hit on an old idea. Typically, web filtering is used to disable user-specified URL addresses or set browser safety for children - restricting access to websites with inappropriate content. Currently, web filtering is used in conjunction with malware scanning tools to increase browser security and content downloaded to users' computers. As you can see, web filtering can instantly give users information about the safety of a website or website.

*** Virus scanning utility on smartphones: At** a conference of Messaging Anti-Abuse Working Group (a non-profit organization with members like Apple, Cisco Systems, McAfee, PayPal and Sprint Nextel), security expert Tim Kaspersky Labs' Armstrong said that the spread of malware on mobile devices is just a matter of time

because hackers have yet to find a way to make money through mobile attacks, but things will change. when smartphones are more widely used in commercial activities. According to the expert, phone security is an issue that needs to be taken care of by users, however, when mobile phones are increasingly integrated with bank accounts and credit cards, security is necessity.