# 5 issues for enterprise security

Sometimes computer users forget the basics of security and create a hole in the process.

**Network administration** - Sometimes computer users forget about the basics of security and create a hole in the process. **With today's limited security budget, you need to make sure you know the highest level of risk issues before going into other issues.**

High-risk problems are not the same but change on a regular basis. Bad guys are still hiding somewhere; The attacks that we find popular today are not the attacks we saw a few years ago. So this article we want to introduce you to the top 5 security solutions that cover the widest range of emerging threats. Many solutions can be considered " *no brainer* " but you will be surprised by the number of companies that do not implement those solutions.

These 5 components are combined well to help prevent many dangerous attacks on data, network and users. There are many other useful security solutions on the market when it comes to choosing the 5 most effective and ready solutions, here are our 5 options:

**Firewalls** - The basic principle in protecting the network for decades still requires a solid grounding security. Its work is still very simple; control flow data. No firewall is set up to block unwanted data streams, and your resource protection work exponentially. Firewalls should be present on the outside perimeter but also needed inside the network to securely segment data. Deploying an internal firewall is a fairly new and good method. Much of it is due to abandoning the notion that the authentication network boundary can distinguish trusted network traffic from unreliable external network traffic. What has changed recently is that firewalls will be smarter and have better control over the definition of data flow. In general, firewalls can now control the flow of data based on the type of application or even the application functionality it represents. For example, a firewall can block SIP voice call data streams based on dialed numbers.

**Router Security (FW, IPS, QoS, VPN)** - Routers are everywhere in most networks. In the past, they used to be like traffic police soldiers to control the flow. However, modern routers can do more work today. They can have a lot of security features, sometimes even more than a modern firewall. Most routers in this area have the features of a powerful firewall, some also have useful IDS / IPS functionality, powerful traffic quality and service management tools, and code features. Virtual Virtual Network data. The list doesn't stop there. The power of modern routers that add to the network security problem is still largely ignored today. With modern VPN technology, users are very simple to encrypt all data in all WAN links, but very few people do so. Besides, not many people use firewall functions and IPS features in their routers. Use it and see how your security situation will improve!

**Wireless WPA2** - If you don't use WPA2 wireless security, stop what you're doing and make a plan to start using them. Many other wireless security methods are not secure enough and can be compromised quickly. Don't make it so easy for bad guys, turn on WPA2 encryption with AES right away.

**Email Security** - We all know that email is now the top target for black hat groups. Viruses, malware, and worms all like to use email as their distribution method. Email is also the way we lose sensitive data. In addition to the top issues in threats and data loss via email, we also have many junk emails and spam. About 90% of emails sent today are spam! A good email security solution will help users remove junk emails and filter out malicious emails. If you receive more spam through your current system, then the chances of you getting malware through it also increase. Therefore the anti-spam feature in email security gateways is the focus, the core percentage of the product. If the product does not perform spam blocking, it certainly cannot catch malware and avoid data vulnerabilities.

**Web Security** - Today's threats from port 80 and 443 are increasing compared to other security threats. Extending the complexity of web attacks requires companies to deploy a robust web security solution. Simple URL filtering has been around for a few years and it must be a core component of web security. However, web security needs more features besides URL filtering, such as AV, malware scanning, authentication IPs, URL sorting techniques and data blocking functions. An attacker can compromise sites with pretty good profiles so if we only rely on filtering whitelists and blacklisting URLs, this method will no longer be safe. Any web security solution must be able to scan dynamic web traffic in order to make a valid decision.

*What do you think about the 5 security options we mentioned in the article? Is that right or wrong? If you want to add a choice, what is your choice?*