Security

Executive brief: When it comes to security, protection and performance matter

Five things your next-generation firewall must do

Introduction

These days, cybercrime is big business. All types of data are being traded, whether it is medical information, credit card information, or the secret designs of your new product, app, or service.

Malware is becoming more sophisticated and today it's commonly hidden inside a larger file, or encrypted so a firewall device can't decrypt it. Meanwhile, the price of cyber-hacking tools is going down, so denial of service attacks, eavesdropping software, and Wi-Fi interception devices are less expensive and more readily available.

Given the maturity and sophistication of malware, businesses of every size and industry are at risk. At the same time, firewalls are becoming more mature and sophisticated, and are better integrated into the network, going beyond security to help improve network efficiency. A high-performing firewall can protect against advanced attacks, as well as control traffic on your network. However, the firewall you had last year probably isn't going to guard you from this year's threats. A firewall has to protect more than assets — it also has to protect people, networks and productivity, and it has to give you granular controls into complex applications.

Given the maturity and sophistication of malware, businesses of every size and industry are at risk.

1. Protect assets and people

Firewalls were originally designed only to secure assets, but modern threats are so much more sophisticated that your firewall must now extend to protecting both assets and people. By functioning as a management hub for people and applications, next-generation firewalls (NGFWs) now allow you to get the type of network performance employees need, so you can get the level of security the business requires. A smoothly running network is one that has blocked spam, which can consume network resources, and restricts non-productive bandwidth-consuming activities such as video downloads.

2. Protect networks

It's easy to have a false sense of security once you install a firewall or cyber-protection program, but too many businesses have learned the hard way that just owning the software isn't enough. Effective network security requires you to enable all program functions, including antivirus detection, intrusion prevention, and content filtering. Firewalls must be able to analyze entire files, including encrypted files and large file sizes. Finally, after the firewall is installed, it's critical that you test it regularly.

3. Protect productivity

NGFWs feature aggressive countermeasures and high-speed performance. This reduces risks, management complexity, and costs, through automated, dynamic security measures that are optimized to protect network performance.

4. Provide granular controls

Firewall control must also be granular enough to manage application functions without disrupting productivity. Firewall zones should also allow you to isolate groups to minimize data leaks or breaches.

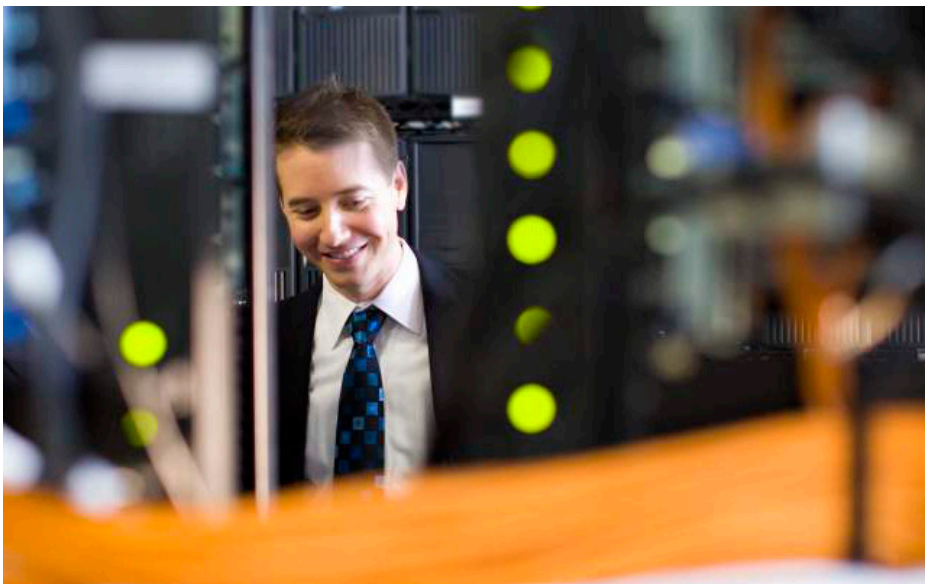
5. Provide scalability and performance

Traditional firewalls often lack the scalability and power to deliver comprehensive protection or the granular control required to keep your organization safe in today's complex, and potentially hostile, IT environment.

Regardless of the size of your business or type of industry, don't let an outdated firewall put your entire business at risk.

Learn more.

Dell offers comprehensive, powerful, next-generation firewalls for organizations of any size. Read our white paper: "How to prevent security breaches in your retail network."



For More Information

About Dell Security

Dell Security solutions help you create and maintain a strong security foundation with interconnected solutions that span the enterprise. From endpoints and users to networks, data and identity, Dell Security solutions mitigate risk and reduce complexity so you can drive your business forward. www.dell.com/security

If you have any questions regarding your potential use of this material, contact:

Dell
5455 Great America Parkway,
Santa Clara, CA 95054
www.dell.com/security

Refer to our Web site for regional and international office information.