Connecting islands or peeling onions:

The challenge of coordinating security resources for maximum impact.

By Ray Boggs, IDC

The deployment of a wide range of technology in midsize firms has transformed operations and improved productivity in a variety of ways. Wireless networks, broadband Internet connectivity, notebook computers, and smartphones have all enhanced the ways employees work, whether working on-site or remotely. The increasing complexity of the technology environment brings with it some real security risks, of course. And typically midsize firms take the mosaic approach to security as they grow, adding a security piece to help support each new technology piece.

While this approach seems effective in terms of cost and ease of implementation, it actually can leave gaps in security coverage that can leave a company vulnerable to accidental or intentional security breaches. Basically the "connect the islands" approach may be OK for smaller businesses, but a more comprehensive vision of security is called for as firms grow.

While small businesses can devote 10% of their total IT budget for security, it increases to about 14% for midsize firms.

Midsize firms are prepared to invest in security, of course, and IDC research indicates that as firms grow they devote an increasing share of total IT spending toward security. While small businesses can devote 10% of their total IT budget for security, that percentage increases to about 14% for midsize firms — and of course that share applies to a total spend that also grows with company size. The nature of that spending also changes, with the mix of hardware, software, and services devoted to security also changing.

Effective security coverage involves a variety of different elements that need to be seamlessly coordinated. Rather than connected islands, a better analogy for your security approach would be an onion with multiple layers. Firms are familiar with endpoint security that protects desktops, notebooks, and smartphones from online threats — antivirus, antispam, anti-spoofing, all the usual threats. This would be the outer layer of the onion. Inside the firewall (another layer) would be a variety of security measures that provide the authentication (are you who you say you are?) and authorization (are you allowed to do what you want to or go where you want to?) that keeps an organization secure.

As a company grows, the different layers of an onion become more important, with the remote and endpoint outer layers of protection surrounding the company's various core network capabilities. Of course things can get complicated, like with email protection which has both network and endpoint implications.

Coordinating and managing the different security elements and layers can place particular demands on midsize firms, which rarely have IT staff dedicated to security. For this reason service providers can play an especially important role, particularly as the storage aspects of security, like data protection and disaster recovery, become essential. While midsize firms spend the largest share of their security budgets on software, with a strong endpoint emphasis, the share spent on services has been growing, especially in North America, Western Europe, and Japan. In those geographies, roughly 20%-25% of security spending is associated with outside services.

Ray Boggs is Vice President of Small/Medium Business and Home Office Research at IDC.
For more information, please visit www.idc.com