Faster-moving attacks threaten enterprises

High speed networks, an exponential increase in the number of endpoints, and a more tech-savvy employee base mean a great deal more risk for enterprises, says Fortinet.

Addressing a media round table in Rosebank, Fortinet Africa executives said the risks to enterprise had increased and changed significantly in recent years. Perry Hutton, Regional Vice President – Africa at Fortinet, pointed out that with high speed broadband, "attackers could empty a Terabyte server in minutes." Wiping and locking down servers for ransom has become commonplace, he said, with one recent local attack wiping 26 servers at once, and at least five known ransomware attacks in South Africa alone in the past week, in an environment where reporting is not compulsory. Thanks to the growth of mobility in the workplace and an exponential increase in the number of IoT devices, the attack surface has also become huge, Hutton said.

Elaborating on the trends informing the release of Fortinet's new operating system, FortiOS 5.4, Hutton noted that very real threats faced businesses of all sizes, in all verticals. "People tend to think only financial services are a target, but this is not the case. Consider the valuable data held by healthcare services, for example. They have extensive personal information about a horde of people, and their networks have literally become borderless, including hospitals, medical insurance companies, healthcare practitioners and patients, and even IP connected medical equipment and patient wearables."

"Disgruntled employees, social engineering and unsecured WiFi networks are the biggest culprits in giving attackers unauthorised access to enterprise data," he said. "This is why internal segmentation is a fantastic solution, because there are some areas of the network where you have to be 300% bulletproof, and other areas where you only have to be 50% bullet proof. You need to make sure that those 300% areas are covered with every resource at your disposal to mitigate that risk as far as possible. You can't take a blanket approach to security anymore."

Fortinet Major Account Manager Paul Williams said connectivity speeds were increasing, and security technology had to keep up. "With connectivity speeds going from 1 to 10 to 100 Gigs and IoT driving the number of connections into the multi-billions, the security has to be ahead of this." System Engineer John Ward said security had to function

at wire speed, offering simplified, full visibility of the network – particularly in enterprises running WiFi networks and managing geographically dispersed branch offices.

“The past few years have seen a dramatic change in how we’ve developed our solutions,” said Williams. “Now we’re delivering the difference between a box that is ‘hanging on by its fingernails’ in a denial of service, and a box that allows visibility and gives administrators the ability to apply rules to mitigate the situation. FortiOS 5.4 adds features like interoperability with our other products, analytic capabilities and assisted one-click actions, and the ability to implement internal segmentation firewalls (ISFW) and Secure Access Architectures to move beyond traditional perimeter defence.”

Hutton added: “There are three rules of security, as far as we are concerned: complexity is the enemy, security is borderless – with the advent of IoT, telecommuting and bandwidth increases this is more the case, and slow is broken.” He emphasized the importance of security to the edge that did not result in complexity or slow down networks with bottlenecks. “It’s crucial to ensure that security is not compromised and that business is able to continue,” he said. “It can seem to be a balancing act for administrators to mitigate against a range of risks. But putting down a myriad security products creates complexity and a massive bottleneck for your traffic. This becomes a massive issue in business today. The answer to these challenges is a security solution that can deliver true network segmentation and full visbility, without compromising network performance.”