Cybersecurity Past and Future: What's Come This Year and What is Coming
By Paul Williams, Country Manager – Southern Africa at Fortinet

You know what they say about history: Those who don't learn from it are doomed to repeat it. Another maxim about the future holds true, too: To predict the future, simply look at the past. With that in mind, here's a quick overview of the current state of cybersecurity, along with what lies on the horizon and what organizations can do to secure their networks.

Mid-Sized Companies and the Cloud
Mid-sized companies are facing a Scylla-and-Charybdis moment with respect to the cloud; it offers huge business benefits but huge risks as well. Research shows that mid-sized firms recently saw higher rates of botnet infections, revealing that these firms deal with more than their fair share of security problems. It is possible that cybercriminals see mid-sized organizations as a "happy medium" because they often do not have the same level of security resources and technologies as large enterprises but still have valuable data assets. At the same time, the attack surface for mid-sized firms is growing at a faster rate than that of larger enterprises due to faster cloud adoption rates.
The cloud continues as a point of vulnerability because its services are centralized and present a huge potential threat landscape. Its complex, hyper-connected networks can produce a single point of failure. Rather than hacking a dozen businesses, criminals can hack a single cloud environment and potentially have access to data from dozens or hundreds of organizations, or wipe out an entire range of services with a single attack. This is the exact scenario by which the Mirai botnet took out a DNS hosting provider.
The success of IoT botnets like Mirai, Hajime and Reaper fuels the prediction that criminals will use artificial intelligence (AI) to detect a weakness and then use it to cripple a service that generates millions of dollars a day for the provider while disrupting service for potentially hundreds or thousands of businesses and tens of thousands or millions of their customers.

The Trouble with Botnets
In the last quarter, many companies experienced the same botnet infections multiple times. This could be due to one of two reasons. Either the organization did not thoroughly understand the total scope of the breach and the botnet went dormant, only to return again after normal business operations resumed, or they never found the root cause or "patient zero."
As unsecured IoT devices become more sophisticated, and attack methodologies become more intelligent, there is the real potential to create swarms of compromised IoT devices that could indiscriminately attack like a hive of angry bees. It is highly probable that cybercriminals will replace botnets with intelligent clusters of compromised devices built around swarm technology to create more effective attack vectors with minimal supervision, or even autonomously.
This would become a hivenet rather than a botnet, and it would be able to use peer-based self-learning to effectively target vulnerable systems at an unprecedented scale. Hivenets will be able to use swarms of compromised devices to identify and tackle different attack vectors all at once. As it identifies and compromises more devices, a hivenet would be able to grow exponentially, widening its ability to simultaneously attack multiple victims.
Intelligent Defences
Security threats like those discussed above demand the latest in security strategies and technologies, but they also require good, old-fashioned cyber hygiene. After all, the best locks on the planet cannot secure a door that's been left open. So then, the first order of business is to identify all your authorized and unauthorized assets within your environment. You have to know what you've got in order to know what you're protecting.
It is also important to limit user privileges; not everyone needs administrator credentials. In addition, keep your assets updated and patched, and limit applications to only those with a business

need. Using unnecessary applications enlarges the attack surface and increases the complexity of protecting the environment.

As for breaches, have a documented plan for how you will detect, analyse, respond to and recover from a breach. Ensure you focus on properly identifying the full scope of the breach and forensics analysis to determine how the threat got there in the first place.

Toward Integrated Security

Finally, the best defence against today's intelligent and automated threats is an integrated, collaborative and highly adaptive security fabric. If you can get the fabric-based security system right, using AI applications such as machine learning, you will have the quintessential security defence system, and will be able to survive this year's threats as well as next year's.