# Endpoint security need to be agile and flexible

Traditional security measures to prevent cyber attacks are falling short, and businesses need a new approach to endpoint security to secure against these ever-present dangers.

©Martin Novak 123RF

"Billions of rands are being spent on traditional endpoint security, and yet companies of all sizes are falling victim to advanced cyber attacks," says Jayson O'Reilly, director of sales and innovation at DRS. He says this is because the majority of today's endpoint solutions are only really geared towards viruses, malware and other malicious code, they are not equipped to handle advanced threats. "They use conventional IPS, anti-virus, anti-spam and similar, which cannot hope to prevent a persistent attack."

Unfortunately, O'Reilly says the attacks are a far cry from the simple and isolated malware attacks a decade ago. "The anatomy of a modern, sophisticated threat is a complex one. It makes use of sophisticated social engineering techniques to get an employee in the target company to click on a link, or it uses stolen login credentials and other techniques to breach the network. Once inside, it lurks about gathering information and exfiltrating data."

## Threat moves laterally

Once the endpoint has been compromised, the threat actor moves laterally, finding other systems and applications to compromise, until they have found the payload they were after, be it proprietary data, blueprints, financial details or similar. "These guys are highly advanced," says O'Reilly. "All they need is a single vulnerability, across the multiple potential attack surfaces. What organisation can hope to protect each and every system and vector with traditional endpoint protection?"

This is where next-generation end-point protection comes in. "Today's endpoint solutions need to be agile, flexible and highly integrated. They need to give a total and far-reaching view of all threats if they have a hope of preventing threats."

There are several elements of an effective, next-generation endpoint solution. "Firstly, it must go beyond signature-based detection and feature advanced detection of previously unknown threats, and this must be able to work within any current security tools that you have. It needs to work with global threat intelligence to pinpoint any anomalous behaviours that might be a tell-tale sign that a breach has occurred."

## Response capabilities

It is also important that it has response capabilities, so that it can validate, contain and remediate to identify if an endpoint is under attack, and if that is confirmed, cease all communications and contain the threat before it spreads and causes major harm.

Another important element is the ability to investigate in a proactive and adaptive manner. "It needs to be able to actively look for threats, and must have forensic capabilities to collect and analyse evidence to see how much damage has been done, how far the threat extends and what, if any, data has been exfiltrated."

Going back to global intelligence, it must be able to sync with cloud and network intelligence sources, and must collect data from around the globe, and from the investigations of known breaches and intrusions, and must share the intelligence with other vendors and researchers to help businesses defend themselves against the procedures, tricks and tools employed by advanced cyber crime networks.

Finally, it needs to be a part of a bigger security picture. "A unified approach to security is needed. Network monitoring, threat intelligence, endpoint protection and next-generation firewalls need to work together, to help security professionals, defend, detect, analyse, respond and mitigate any advanced threats."