Get Real-time unknown malware prevention through Westcon-Comstor

By Denan Erasmus, channel manager Palo Alto Networks and Firemon at Westcon-Comstor Southern Africa

Many companies deploy various security products and software agents on their endpoint systems, including one or more traditional antivirus products. However, cybersecurity breaches continue to increase in variety and sophistication.

Traps Advanced Endpoint Protection from Palo Alto Networks takes a step forward by combining the most effective, purpose-built malware and exploit detection methods to prevent known and unknown threats before they can successfully compromise an endpoint.

By focusing on detecting and blocking the techniques at the core of these attacks, Traps can prevent sophisticated targeted attacks as well as new types of attacks meaning that all known and unknown threats are prevented. In the industry this is called Zero Day attacks.

As a component of the Palo Alto Networks Next-Generation Security Platform, a natively integrated and automated platform designed to safely enable applications and prevent cyber breaches, Traps shares and receives threat intelligence information from the Palo Alto Networks WildFire cloud-based malware analysis environment.

Threat intelligence information is passed to WildFire by each component of the security platform, and Traps uses this information to block threats to the endpoint no matter where they originated.

Westcon-Comstor Southern Africa resellers and customers can leverage Traps' new functionality, which includes static analysis via machine learning and trusted publisher capabilities to detect and immediately stop malware that has never been seen before.