

Aussie ContentKeeper boosting internet security

Communications Day

Issue 3219

Tuesday 26 February 2008

Sonia Han

Canberra based ContentKeeper has announced the availability of a new internet security technology in its Internet content filtering products that identifies malicious code travelling inside SSL & TLS sessions. It is claimed to be the first one of its kind from an Aussie company.

Malicious code is a technique used by hackers and cyber criminals to steal financial and other confidential information.

The new technology features 'deep packet inspection', which identifies and inspects the contents of a SSL package for malicious code, before alerting the IT administrator. Combined with commonly used approaches such as 'white lists' and 'certificate checks', ContentKeeper's triple-layered approach increases detection rates.

"Without a presence inside the SSL stream, security administrators have no control over all the data that flows in and out of their networks. This technology allows legitimate trusted connections to pass through without decryption; while a non-trusted connection, such as malicious code, can be decrypted, analysed and blocked, before reaching its target and cause a security breach," said Nathaniel Wieriks, senior security engineer at ContentKeeper.