ContentKeeper and Cylance Ink OEM Agreement to add Predictive Malware Blocking to ContentKeeper's Multi-layered Gateway Security Platform

CANBERRA, AUSTRALIA – September 7, 2017 – ContentKeeper Technologies and Cylance® Inc. have signed an original equipment manufacturer (OEM) agreement to embed the Cylance OEM Engine into ContentKeeper's Multi-layered Gateway Security Platform. The new ContentKeeper Predictive Malware Blocking engine will add artificial intelligence-driven, pre-execution malware blocking to ContentKeeper's Multi-Layered Gateway Security Platform that delivers a powerful combination of innovative security technologies to prevent malware and advanced persistent threats.

"Cylance's innovation and vision to provide the next level of security automation is well-aligned with our gateway security platform approach. The speed and accuracy in which the technology analyzes and identifies advanced threats and malware is unparalleled in our industry. We look forward to helping organizations streamline and scale their security defenses," said David Wigley, CEO at ContentKeeper.

ContentKeeper's Gateway Security Platform is a multi-layered malware defense system that unifies multiple critical security functions into a single cohesive, easy to manage next-generation solution. Predictive Malware Blocking will provide an advanced level of malware protection beyond the signature-based antivirus pattern-matching technology currently used.

"At Cylance, we're dedicated to delivering artificial intelligence/machine learning wherever possible, since current technology can't keep up with today's mutating malware. ContentKeeper's Multi-layered Gateway Security Platform is a natural fit," said Craig Whetstone, Director of OEM at Cylance. "Now, ContentKeeper customers can proactively block targeted attacks using Predictive Malware Blocking as part of a comprehensive, integrated solution that's been proven around the world."

About the Cylance OEM Engine

Cylance OEM Engine is an embeddable malware detection technology that uses Cylance's predictive models to classify files as good or bad by correlating them with the features found in millions of good and bad samples. Its models detect even zero-day and previously unknown malware not in the original training set. Instead of using manually-created signatures, the Cylance OEM Engine computes a "confidence score" for every sample it processes. It also checks for various capabilities that are prevalent in malware and provides a threat indicator report to explain the classification. For example, the report will call out the capabilities of executable, such as logging of keystrokes, ability to inject code or terminate other processes, ability to tamper with a firewall policy, etc. This provides a helpful data point to accelerate further analysis and response to detected threats.

About ContentKeeper

ContentKeeper helps secure enterprises, educational institutions and government agencies worldwide. Our Multi-layered Gateway Security Platform delivers a powerful combination of innovative security technologies enabling today's distributed, cloud-based organizations to protect their networks, users and data from cyber threats. To respond to evolving threats, a growing mobile workforce and the rapid pace of business, ContentKeeper's mission is to develop the world's most innovative, high-speed web security platform, protecting valuable assets today and in the future. The company is headquartered in

Canberra, Australia and maintains U.S based operations in Anaheim, California. For more information, visit www.contentkeeper.com.

Media Contact

Alison Norris
ContentKeeper
(714) 801-9355
alison.norris@contentkeeper.com

###