Trend Micro TippingPoint, Powered by XGen™ Security, First to Infuse Machine Learning Capabilities into its Next-Generation Intrusion Prevention System

Trend Micro Network Defense brought to new levels of smart detection and rapid response

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today announced the latest enhancements to its network defense solutions, leveraging the company's powerful XGen™ security. Continuing its smart, optimized and connected security strategy, Trend Micro has infused patent-pending machine learning capabilities into its Trend Micro™ TippingPoint next-generation intrusion prevention system (NGIPS) solutions. This makes Trend Micro the first standalone NGIPS vendor to detect and block attacks in-line in real-time using machine learning.

TippingPoint NGIPS is part of the Trend Micro Network Defense solution which, in combination with advanced threat protection, is optimized to prevent targeted attacks, advanced threats and malware from embedding or spreading within a data center or network. Network Defense is powered by XGen™ security, a blend of cross-generational threat defense techniques specifically designed for leading customer platforms and applications and fueled by market-leading threat intelligence.

"Protecting an enterprise network is a vital part of a connected threat defense that should also include servers and endpoints," said Steve Quane, executive vice president and chief product officer for Trend Micro TippingPoint. "As businesses grow, the need is greater to have a solution that can provide visibility and control within any customer environment while sharing threat intelligence across security layers."

Trend Micro TippingPoint NGIPS applies machine learning statistical models to feature vectors extracted from network data on the wire to make a real-time decision on whether network traffic is malicious or benign. This evolution helps to better detect advanced malware behavior and communications invisible to standard defenses. TippingPoint NGIPS also applies machine learning techniques to detect and block known and unknown malware families that use domain generation algorithms (DGAs) to generate domain names for infected hosts attempting to contact their command and control servers.

"Our enterprise clients inquire regularly about the need to protect their networks from existing and emerging threats," said Andrew Braunberg, managing director of research for NSS Labs. "Enterprises are continuing to deploy NGIPS devices, particularly to protect high value assets, such as data centers. Advanced analytics, such as machine learning, and fully integrated global threat intelligence feeds are particularly important features for today's leading NGIPS products."

"With the addition of machine learning capabilities into the TippingPoint solution, we have been able to improve the accuracy of detecting malicious activity, which speeds up protection of our network across our business," said Erwin Jud, senior security engineer for SBB AG – Swiss Railways Ltd. "When you blend that with exclusive vulnerability data, not only is my administrative security management reduced, but I feel confident that I have the most advanced threat techniques that continue to adapt now and in the future to keep my company's data secure."

One of the distinguishing features of Network Defense is preemptive threat prevention between discovery and patch availability for many known and undisclosed vulnerabilities. The Zero Day Initiative brings exclusive insight into undisclosed vulnerability data, which results in protection for customers 57 days on average before a vendor can provide a patch. When combined with the security intelligence from TippingPoint Digital

Vaccine® Labs (DVLabs) and data collected from the Smart Protection NetworkTM for threat correlation, each delivers unparalleled, real-time, accurate network threat insights. Information is seamlessly shared with security information and event management (SIEM), gateways, as well as both Trend Micro and third-party security investments.

TippingPoint NGIPS offers in-line comprehensive threat protection against advanced and evasive malware across data centers and distributed enterprise networks. It offers in-depth analysis of network traffic for comprehensive contextual awareness, visibility and agility necessary to keep pace with today's dynamic threat landscape.

In October 2016, Trend Micro TippingPoint NGIPS received a “recommended” rating in NGIPS testing from NSS Labs. For more information about TippingPoint solutions, please visit http://www.trendmicro.com/tippingpoint.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 5,000 employees in over 50 countries and the world’s most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud. For more information, visit www.trendmicro.com.

Contact:

Trend Micro Incorporated
Jerrod Resweber, 972-499-6614
publicrelations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY
