Trend Micro IoT Security 2.0 Enhances End User Protection and Device Makers’ Reputation

Latest version of IoT security platform improves protection, visibility and control

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today announced the global launch of Trend Micro IoT Security (TMIS) 2.0 to help manufacturers and managed service providers improve the security of their products and the wider IoT ecosystem, while enabling them to drive competitive differentiation.

With most traditional security products, it’s not possible for end users to install protection for IoT solutions by themselves, which is where TMIS 2.0 comes in.

“IoT threats are no longer theoretical: endpoints around the globe are being hijacked for data theft, attacked with ransomware and crypto-mining malware, conscripted into DDoS botnets and more,” said Akihiko Omikawa, executive vice president of Trend Micro. “It’s vital that manufacturers step up to raise the bar on security. By integrating threat monitoring, detection and protection into the device itself, consumers and businesses will enhance their security from the moment they install and switch on TMIS 2.0. That’s the kind of value the market is increasingly demanding of IoT device makers.”

The TMIS 2.0 platform can be pre-installed onto IoT devices during the product development lifecycle, requiring minimum deployment effort and providing maximum protection through a range of system hardening and risk detection features.

This updated version offers tight integration with Trend Micro’s industry-leading threat intelligence platform the Smart Protection Network to offer a Web Reputation Service and IoT Reputation Service which block visits to malicious URLs/websites.

The improved installation script makes integration easier for device makers and IoT MSPs, and provides new capabilities to automate security learnings for these firms with less operational effort.

Reports on vulnerabilities, virtual patch deployment and more are emailed to administrators and device makers to provide more flexible management capabilities. A security detection log is stored locally and can be accessed by the device maker for each specific purpose (e.g. to show red light on the device). TMIS 2.0 also boasts an offline mode and proxy support for a wider range of networking environments.

All of these enhancements come alongside the product’s comprehensive range of security capabilities: Application Whitelisting, Hosted Intrusion Prevention Services (HIPS), and System Vulnerability Scanning.

Together, they work to reduce the device attack surface, ensure firmware integrity and block active attacks — minimizing cyber risk for the end customer but also keeping device maintenance costs as low as possible while burnishing the corporate reputation of the device maker/MSP.

More information of Trend Micro IoT Security, please visit: Trend Micro IoT Solutions

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 workloads, networks, and endpoints. With more than 6,000 employees in 50 countries and the world’s most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. For more information, visit www.trendmicro.com.

Contact:

Kateri Daniels
817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY

---

https://newsroom.trendmicro.com/2019-01-09-Trend-Micro-IoT-Security-2-0-Enhances-End-User-Protection-and-Device-Makers-Reputation