

## **Trend Micro Enhances Protection for Air-Gapped Industrial Control Systems**

**New USB device delivers security and operational excellence for critical environments**

**DALLAS, Nov 4, 2021** – [Trend Micro Incorporated](#) (TYO: 4704; TSE: 4704), a global cybersecurity leader, today announced a new portable security device designed to scan for and clean up malware on isolated industrial control systems (ICS), as well as to provide secure storage and data transfer.

***To find out more about the Trend Micro Portable Security™ 3 Pro Edition (TMPS3 Pro), please visit: [https://www.trendmicro.com/en\\_us/business/products/iot/industrial-endpoint-security/portable-security3.html](https://www.trendmicro.com/en_us/business/products/iot/industrial-endpoint-security/portable-security3.html)***

"Some of the world's most critical industrial facilities feature air-gapped ICS machines to minimize the risk of compromise. Flash drives are commonly used to transfer data in an air-gapped environment, but it creates a risk of insider threat," said Akihiko Omikawa, executive vice president of IoT security for Trend Micro and chairman of TXOne Networks. "Our answer is the TMPS3 Pro, developed by Trend Micro's OT-focused subsidiary TXOne Networks. This is a device similar to a USB flash drive that combines malware scanning and removal with secure storage for the first time. It's a one-stop-shop for industrial system security teams."

TMPS3 Pro performs malware scanning on target devices during regular maintenance. It also offers secure storage, allowing worry-free file transfer between different working environments to help ensure industrial control systems stay secure. All files stored in secure storage will be scanned and encrypted on the fly with its AES-256 encryption engine.

As well as reducing breach and compliance risk, the device offers the following benefits:

- Zero installation – performs on-demand malware scans on any system without software installation
- Easy to operate – combines malware scanning/removal and secure storage in one device to reduce operational burden on security teams
- OT visibility – collects computer information, Windows Update status, application lists, and more from systems that were previously a black box, eliminating shadow OT
- Centralized management – offers an integrated view of scans across multiple devices and endpoints

As threats from hostile nations and financially motivated cybercrime gangs mount, ICS security comes under increasing scrutiny from governments and regulators.

In the US, the Biden administration launched an Industrial Control Systems Cybersecurity Initiative in April, which began with a [100-Day Action Plan](#) for the electricity sub-sector, and has since been expanded [to gas pipelines](#).

Meanwhile, the European Union published [an updated draft version](#) of its NIS Directive in December 2020, which will mandate that providers of critical infrastructure services comply with a new range of cybersecurity requirements.

### **About Trend Micro**

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and

central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. [www.TrendMicro.com](https://www.trendmicro.com)

---

<https://newsroom.trendmicro.com/2021-11-4-Trend-Micro-Enhances-Protection-for-Air-Gapped-Industrial-Control-Systems>