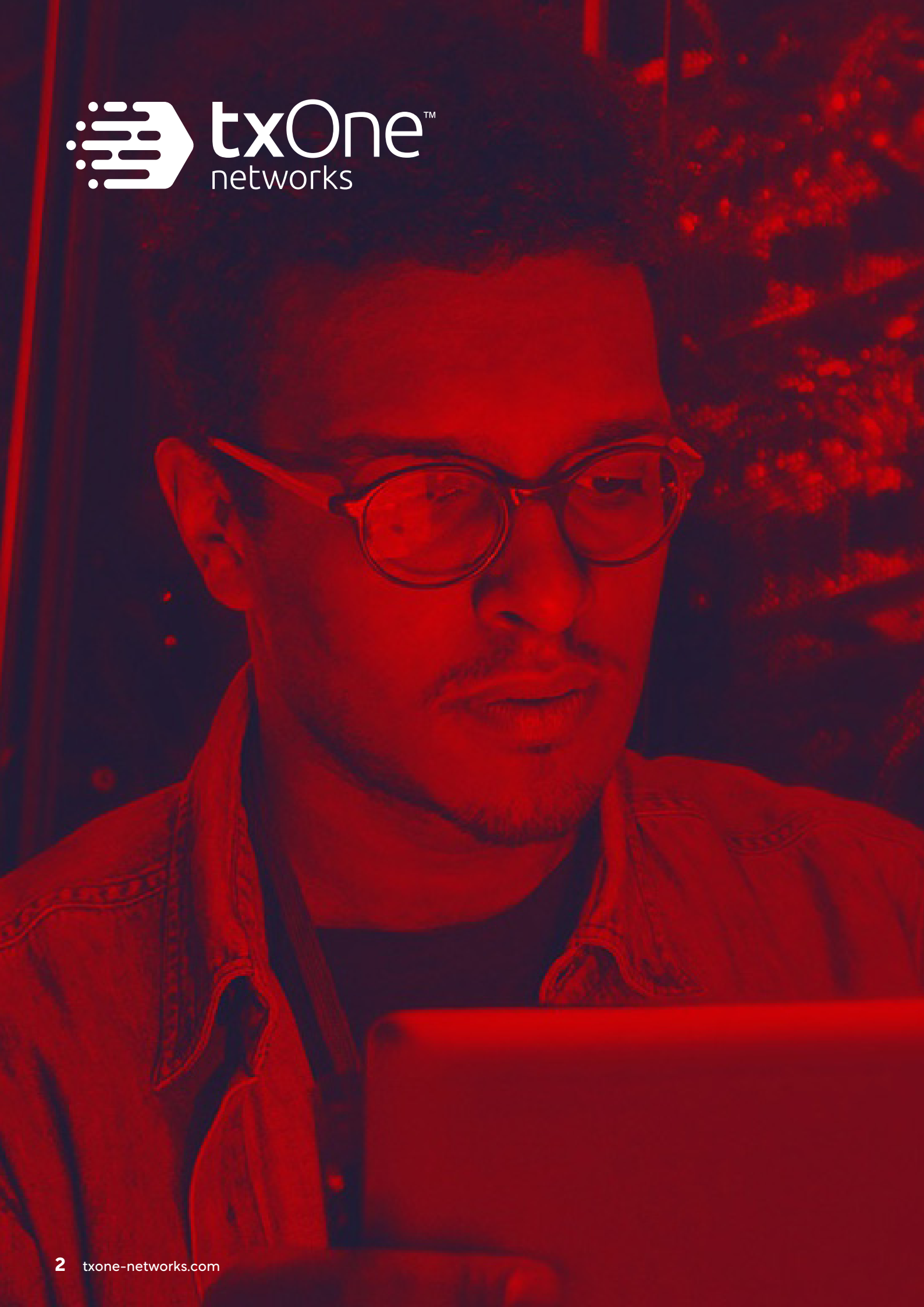
txOne networks

Reduce the Threat Landscape for your ICS

DIGITAL REPORT 2021

IN ASSOCIATION WITH:

Atos


txOne™
networks

Reduce the threat landscape for your **ICS**

“If you have a profitable manufacturing business, you will be targeted by hackers”

Dr. TERENCE LIU
CEO OF TXONE NETWORKS,
VICE PRESIDENT OF TREND MICRO

TXOne Networks delivers convenient and reliable cybersecurity for the era of IT-OT convergence

If you have a profitable manufacturing business, you will be targeted by hackers." This is the stark warning given by Dr. Terence Liu, CEO of TXOne Networks and Vice President of Trend Micro. For more than two decades Liu's single-minded pursuit has been the eradication of cyber risk to industrial control systems (ICS).

During a year in which we saw ransomware attacks on both the Colonial Pipeline, which supplies 45% of the US East Coast's fuel, and JBS Foods, the world's largest meat supplier, President Joe Biden has released a call to action for large-scale improvements to ICS cybersecurity - a call which has been answered by TXOne Networks.

Speaking from his office in Taipei, Taiwan, Liu discusses the importance of adaptive cybersecurity for ICS shop floor protection and shows how this can be achieved from network to endpoints with maximised operational integrity for both legacy and modernised assets.

Cybersecurity is the practice of protecting systems, networks, and computer programs from digital attacks in which hackers seek to change or destroy sensitive information, extort money from targets, or disrupt business activities. Hackers are

becoming increasingly innovative in their targeted attacks on OT systems, which is why TXOne Networks works with global manufacturing clients from a wide range of specialisations including smart factories, the oil and gas sector, healthcare, and other critical infrastructure sectors to ensure there are no disruptions to critical missions.

Mitigation of cyber risks

Since their founding in 2019, TXOne has focused on using customised technology to mitigate cyber risk in connected industrial settings.

"Our solutions are natively designed to fit a manufacturer's needs and special environments. They fit seamlessly into daily operations, becoming part of standard operating procedures. Cybersecurity is fabricated into your daily operation. It's not like an IT security product being put into OT – this is why manufacturers adopt TXOne products on their shop floor and in their plants," commented Liu.

"We listen to the needs of leading manufacturers and critical infrastructure operators to develop the best actionable approach to OT cyber defence. This allows us to create customised technology that

goes beyond traditional security tools to mitigate the complex challenges of securing modern work sites.

"Given that ICS environments are layered and composed of a variety of equipment in different operating systems, TXOne Networks offers both network-based and endpoint-based products to secure the OT network and mission-critical devices in a real-time, defence-in-depth manner.

"Both IT and OT can have comprehensive visibility of ICS assets, protocols, control commands, risks, and threats. The goal is not only to maximise ICS protection, but also to keep the business and operation running

EXECUTIVE BIO

Dr. TERENCE LIU

TITLE: **CEO OF TXONE NETWORKS, VICE PRESIDENT OF TREND MICRO**

INDUSTRY: **CYBERSECURITY**

LOCATION: **TAIWAN**

Dr. Terence Liu is the CEO of TXOne Networks, a subsidiary company of Trend Micro. TXOne Networks brings pragmatic and practical OT cyber defence to the industrial world by integrating Trend Micro's security technology and Moxa's ICS hardware and experience. As a vice president of Trend Micro, Liu also leads Trend Micro's Network Threat Defense Technology Group, where he focuses on developing and marketing distributed security solutions across the telecommunication infrastructure by leveraging new-generation telecommunication technologies like Software Defined Networks (SDN) and Network Function Virtualisation (NFV). Prior to this Liu was the CEO of BroadWeb. He defined its DPI licensing business and led profitability for five years in a row. BroadWeb was acquired by Trend Micro in October 2013.

Smart Factory.
Smart Defense.
Digital Security for Manufacturing.

Manufacturing is a lucrative target for cybercrime. As a large industry with valuable data and a growing IoT attack surface, your data is of direct value to hackers.

Learn more

Atos

even when security is threatened. Hackers will pick the most profitable manufacturer or enterprise to attack. If your business is profitable and successful sooner or later they will come for you. You need to be prepared and protected."

Heightened risk from pandemic

According to Liu, the current pandemic has shifted the security landscape considerably and introduced many new risks leaving the door wide open for malicious adversaries.

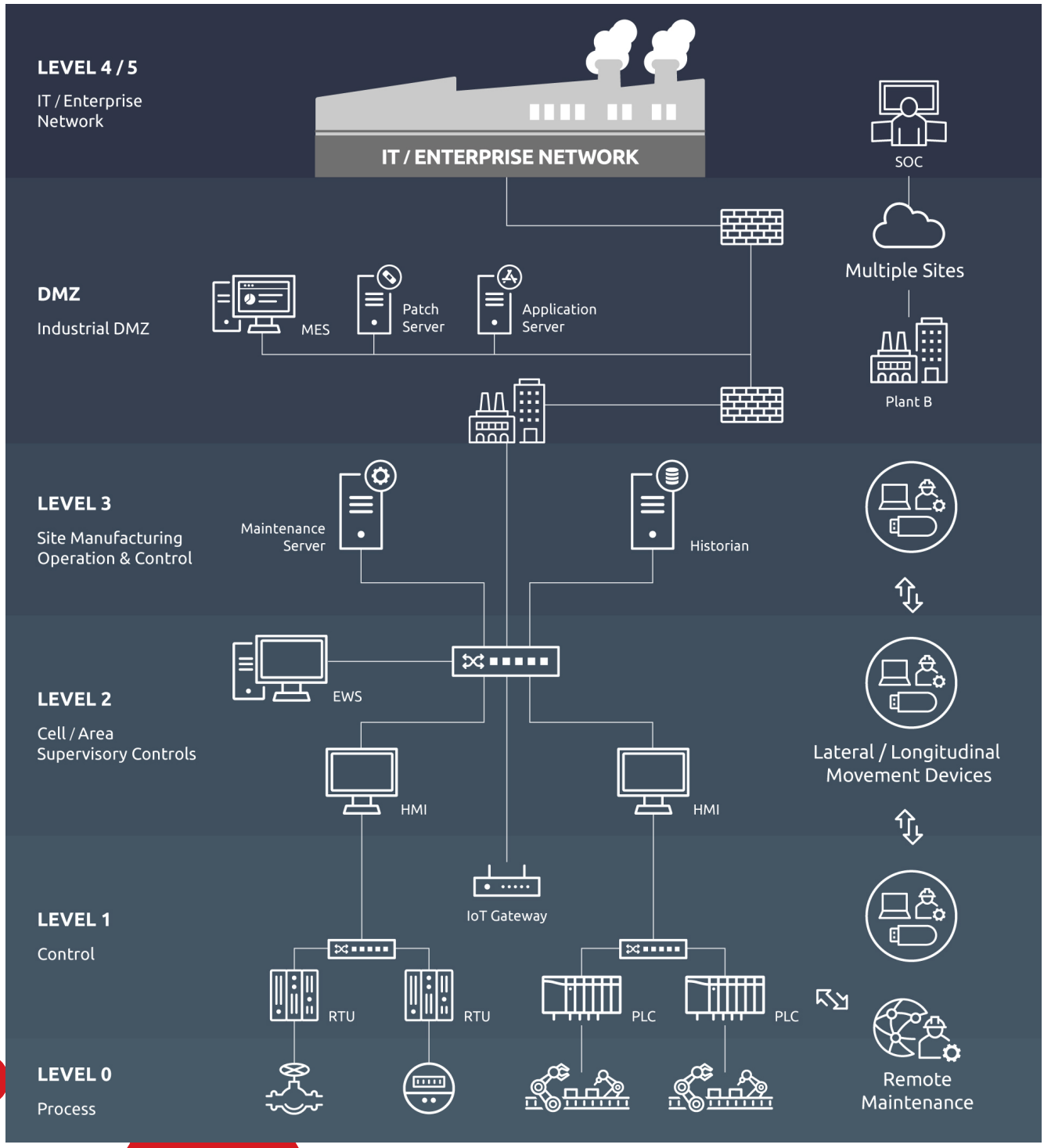
"When the hackers get into the system, they have the ability to cause a catastrophe or even cause injury – this makes cybersecurity much more important"

Dr. TERENCE LIU
CEO OF TXONE NETWORKS,
VICE PRESIDENT OF TREND MICRO

"The cybersecurity world has fundamentally changed. Prior to COVID-19, a manufacturer could rely on physical help for the machines on their shop floor. Now, such help is delivered through remote diagnostics which may have to be accessed through the internet.

"When you open the door to that technician, you also open the door to hackers – actually, it's the same door. If hackers decide to target your company, they'll return again and again trying to find a way into your network, and if they're successful then not long after that the key to your door will be available for sale on the internet. Another group of hackers will leverage that information to get into your system, implant ransomware, exfiltrate sensitive data, and demand money for its return."

"Manufacturers need to think more about the process of creating protection, and how to have a secure way for your vendors or technicians to be able to access your system. That's a challenge for companies who don't have a good defensive strategy in place.



Portable Security™ 3 makes it easy for ICS owners & operators to scan for malware on standalone computers

TXOne ICS Cybersecurity Deployment Architecture

"Since the pandemic, manufacturers need to think about how they're making their systems more automated. As new technology makes factories more automated, we don't need as many technicians or employees on site – but that automation also makes cyber attacks easier to conduct. Added convenience and control for personnel is turned into added convenience and control by intruders. When the hackers get into the system, they have the ability to cause a catastrophe or even cause injury – this makes cybersecurity much more important."

Research into cyber threats is crucial to educating the public and strengthening the defensive tools that help combat threat actors and attacks. TXOne Networks is supported by R&D and security research teams based in their US and Taiwan offices, as well as business development managers and subject matter experts working all over the world.

Three TXOne Network solutions for ICS environments:

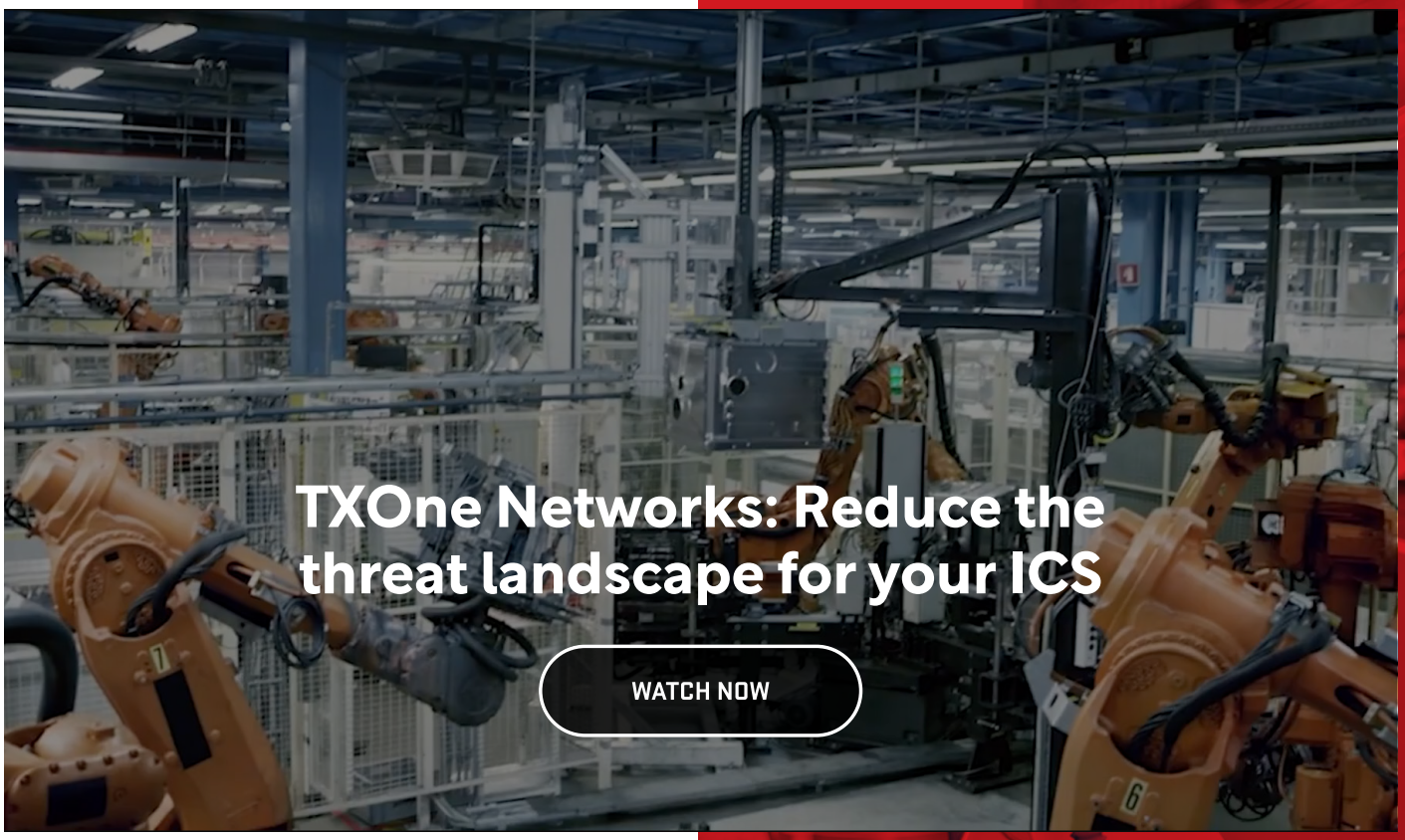
1. Endpoint protection

Modern work sites usually need to accommodate legacy endpoints in their operational environment, which must be able to interconnect and work with their different assets.

"Traditional antivirus is not designed for the ICS environment – constant virus signature updates depend on an internet connection while intrusive file scans take up a lot of processing power and can easily interfere with operations," comments Liu.

"ICS endpoint protection requires a different spectrum of consideration. Security must never jeopardise routine operation, slow down computation, or delay decisions made in the factory production process."

TXOne Networks offers adaptive, all-terrain ICS cybersecurity solutions in the



form of different endpoint suites that secure both legacy systems and modern devices in a variety of work site environments, customized with input from leading specialists in each vertical.

2. Network defence

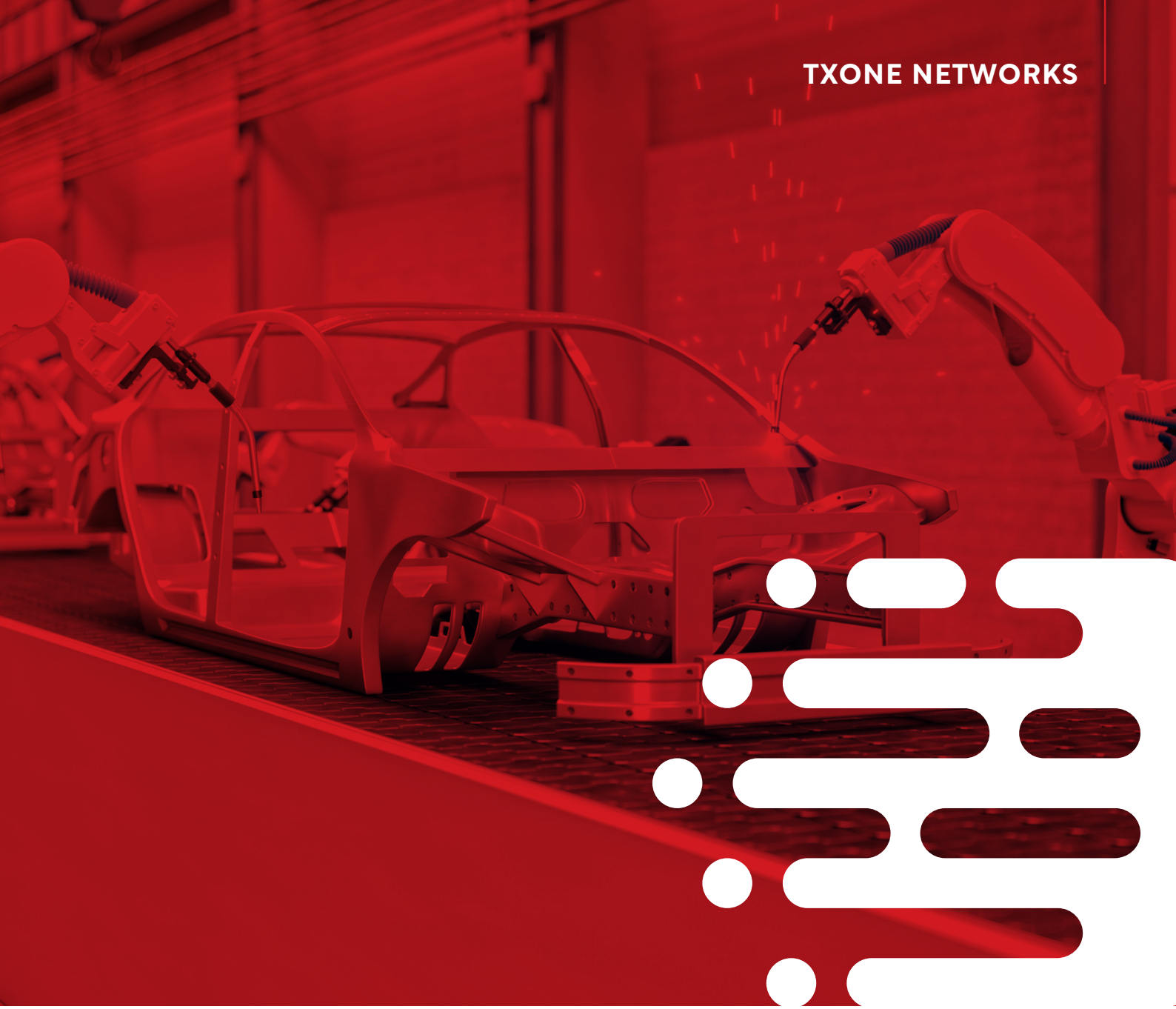
Cyber attacks can spread through an OT network lightning-fast, creating a catastrophe with a price tag numbering into the millions of dollars. Unpatched and legacy assets are usually essential to operations, and they require specialised protection that safeguards and maintains productivity.

"TXOne Networks' adaptive ICS cybersecurity solutions are specifically designed to create a safe, reliable work environment even for the most sensitive or essential technologies, keeping the operation running," said Liu.

"Virtual patching shields unpatchable or legacy devices and network segmentation mitigates risk by making the network fundamentally more defensible while advanced ICS protocol-based trust list profiling gives granular, highly-detailed control over assets. These have been worked into industrial-grade ISIPS (Internal Segmentation IPS) appliances purpose-built for any business intention."

3. Security inspection

Continuity of security inspections is integral to a modern work site defense plan. "Without



routine security inspections personnel, process, and technology are all vulnerable," comments Liu. "The correct solution for scanning and clean-up streamlines the necessities: supply chain security auditing, inspection of all devices that visitors bring on-site, and checkups for air-gapped assets.

"TXOne Networks' Trend Micro Portable Security 3 offers a USB form-factor easy for non-experts to use, with LED lights that show the inspection result after scanning Windows or Linux devices. To eliminate the shadow OT, asset information will be collected during every scan and sent to the central management console where it's easily reviewed and archived. This installation-free device's portability and user-friendliness is tailored to the fast-moving needs of ICS environments and fits in the palm of your hand."

Partnership with ATOS

TXOne Networks began as a joint venture by "cyber giant" Trend Micro, which has more than 30 years of experience in cyber defence, and Moxa, who provide industrial networking products.

"Having Trend Micro and Moxa on board allows us to leverage their technology and knowledge so that we can create ideal solutions for operational environments," said Dr. Liu. Commenting on their partnership with ATOS, Liu said: "Our host, ATOS, has a

QUICK FIRE QUESTIONS:

Dr. Terence Liu, CEO of TXOne Networks, Vice President of Trend Micro

Why should a smart factory adopt TXOne Networks solutions?
"Manufacturers should adopt TXOne Networks solutions because we offer native cybersecurity technologies developed for manufacturers and critical infrastructure operators to make sure they can be seamlessly integrated into your operation."

What do you consider to be the biggest cybersecurity threats in 2021/22?
"Targeted ransomware and double extortion are two of the biggest security threats right now, and potentially devastating supply chain attacks will be one of the main attack methods during the next two years."

What is the biggest mistake a company makes when looking at cybersecurity?
"A company should be able to segment their infrastructure into small networks, have streamlined routine inspections, and make sure their east-west traffic is clean."

What technology are you most excited about in the future when it comes to enhancing cybersecurity?
" Artificial Intelligence and machine learning will be significant technologies for creating more manageable workflows and reducing alert fatigue in SOCs (Security Operation Centres). We also expect increased accuracy from XDR (Extended Detection and Response) platforms to ensure early breach detection and that the ideal response is chosen."

"Our solutions are natively designed to fit a manufacturer's needs and a spatial environment. They can seamlessly fit into the operation and become the standard procedure"

Dr. TERENCE LIU
CEO OF TXONE NETWORKS,
VICE PRESIDENT OF TREND MICRO

fantastic relationship with Trend Micro. "We work closely with ATOS, who have partnered with us to make our products available in Europe."

Competitive edge

"I think TXOne Networks is in a very unique situation," said Liu. "When companies began trying to do industrial cybersecurity, they started from providing asset management, because if you founded a cybersecurity company for OT 10 years ago people didn't have the anxiety that they do now – they just wanted visibility.

"TXOne Networks was founded in 2019 at the right time, when the spotlight was shining on OT. Cybersecurity has three stages – you find, you identify, and then you protect. We've focused on providing streamlined, ICS-tailored protection to our customers," said Liu, who admitted that while the pandemic may have slowed the pace of development for some start-ups it had set off a significant increase in the need for OT cybersecurity.

"Our competitive advantage is that our solutions are natively designed for the world of OT and the ability to work with a full modern control system – our competition takes their IT-based product, puts it into ruggedized hardware and calls it OT security, but to us there is a huge difference. OT stakeholders need solutions specially adapted to their environments and daily work. This is especially true for the different OT verticals, which often have different mission-critical needs. Our ability to adapt to the potentially fragmented OT environment and provide OT-native cybersecurity products is our main difference," said Liu.

11F, 198, Sec. 2,
Tun Hwa S. Rd
Taipei 106,
Taiwan, R.O.C.

T 886 2 23789666
txone-networks.com

POWERED BY:

BMG BizClik Media Group