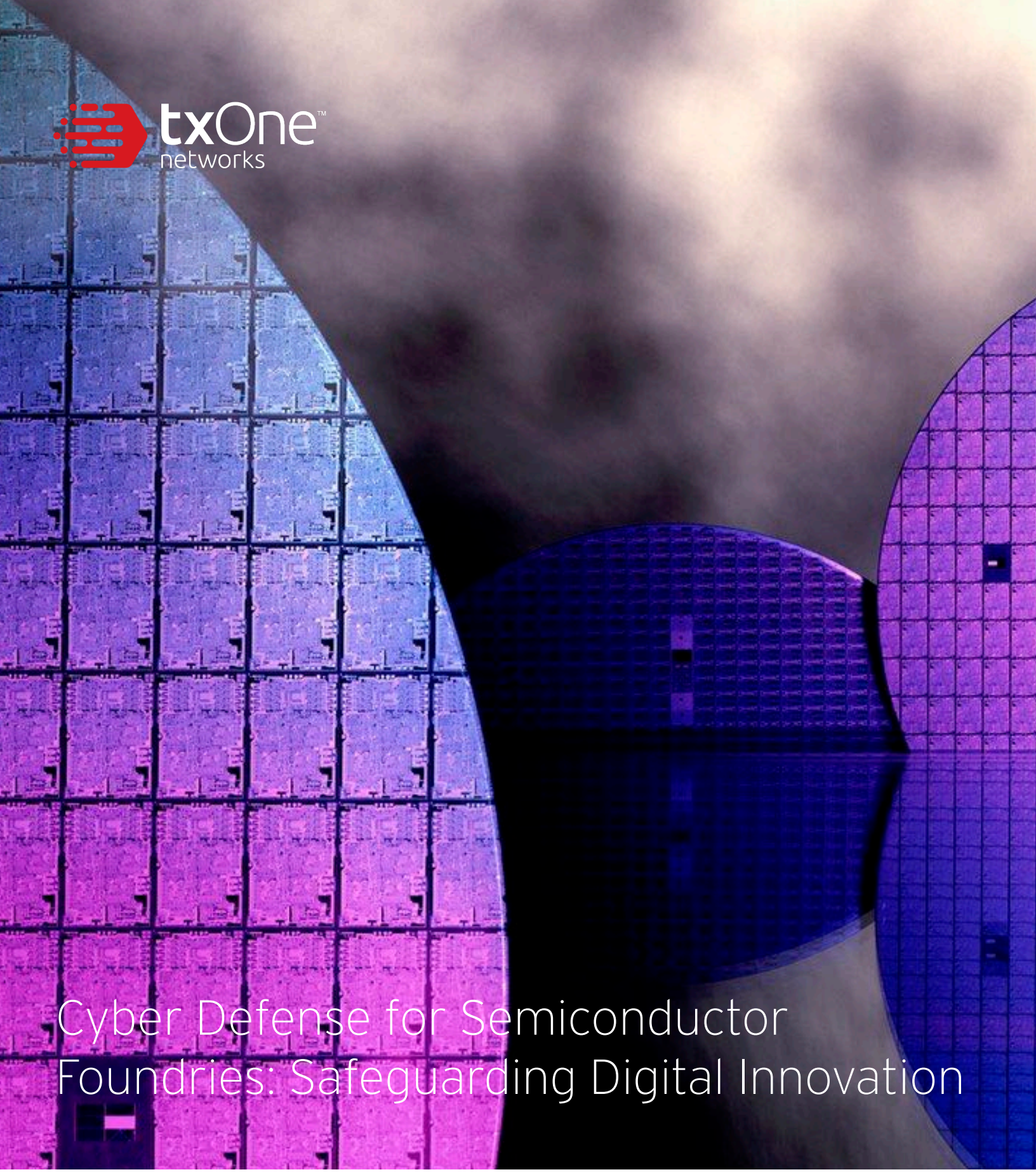
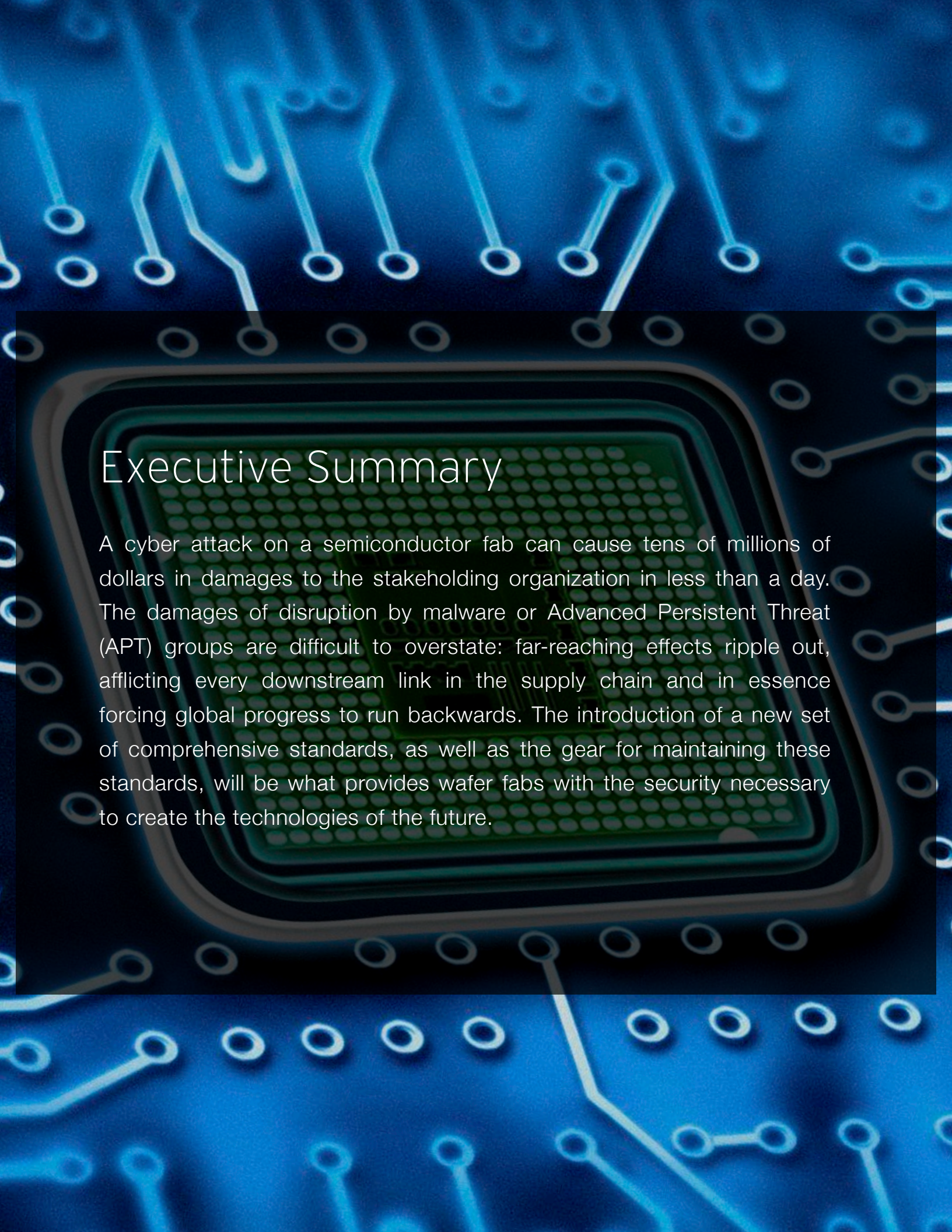


# Cyber Defense for Semiconductor Foundries: Safeguarding Digital Innovation

TXOne Networks Inc.

Ryan Lung, Hsien Wei Hung, Max Farrell

# Table of Contents



# Executive Summary

A cyber attack on a semiconductor fab can cause tens of millions of dollars in damages to the stakeholding organization in less than a day. The damages of disruption by malware or Advanced Persistent Threat (APT) groups are difficult to overstate: far-reaching effects ripple out, afflicting every downstream link in the supply chain and in essence forcing global progress to run backwards. The introduction of a new set of comprehensive standards, as well as the gear for maintaining these standards, will be what provides wafer fabs with the security necessary to create the technologies of the future.

# Incident Overview

Attacks on semiconductor manufacturers such as X-Fab and Tower Semiconductor in 2020 brought wafer fabs to a complete stop for days and affected production for weeks. These cyber attacks can result in tens of millions of dollars in losses while systems are being restored – the TSMC attack in 2018 cost $85 million USD. In some of these attacks, data is successfully protected from being locked or exfiltrated, while in others it is not – exfiltrated data is typically flipped onto the internet to aid in extortion tactics.

## X-FAB

On July 5, 2020 Maze ransomware was leveraged in a targeted attack on the infrastructure of X-FAB, a company famous for their analog and mixed-signal semiconductor applications.[1] Production was halted at the organization's six factories, and hackers released a small piece of stolen data on the internet in an attempt to extort money from stakeholders. One of their sites was announced to have resumed production by July 13, 8 days later, with other sites resuming production within another week.

## Tower Semiconductor

The cyber attack on Tower Semiconductor shut down all 7 of their manufacturing sites for days as it spread globally between factories in Israel, the U.S., and Japan to cause an immediate 1.3% drop in stock value.[2] The attack took place on Sept. 6, with work sites back online by Sept. 10, however the attack cost "between 8-12 days of missed new wafer starts … [as well as] multiple weeks of full fab activity levels."[3] Further details of the cyber attack's financial effects were not released. No organization stepped out to claim responsibility for the attack.

---

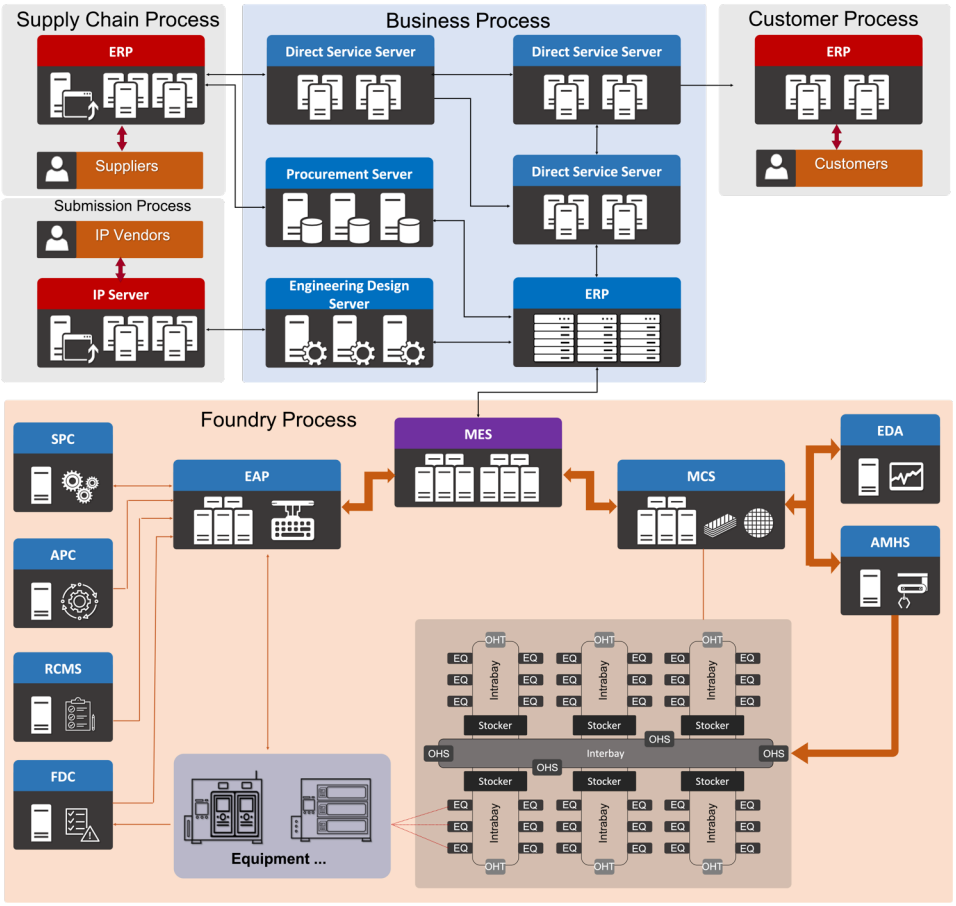
[1] Sam Varghese, "Texas foundry group X-FAB takes a hit from Maze ransomware", July 16 2020

[2] CISO MAG, "Israel's Tower Semiconductor Hit by a Cyberattack", Sept. 8 2020

[3] Migdal Haemek, "Tower Semiconductor Reports Third Quarter 2020 Results and Guides Fourth Quarter Significant Revenue Increase", Tower Semiconductor, Nov. 12 2020

# Securing the Most Complex Production Cycle On Earth

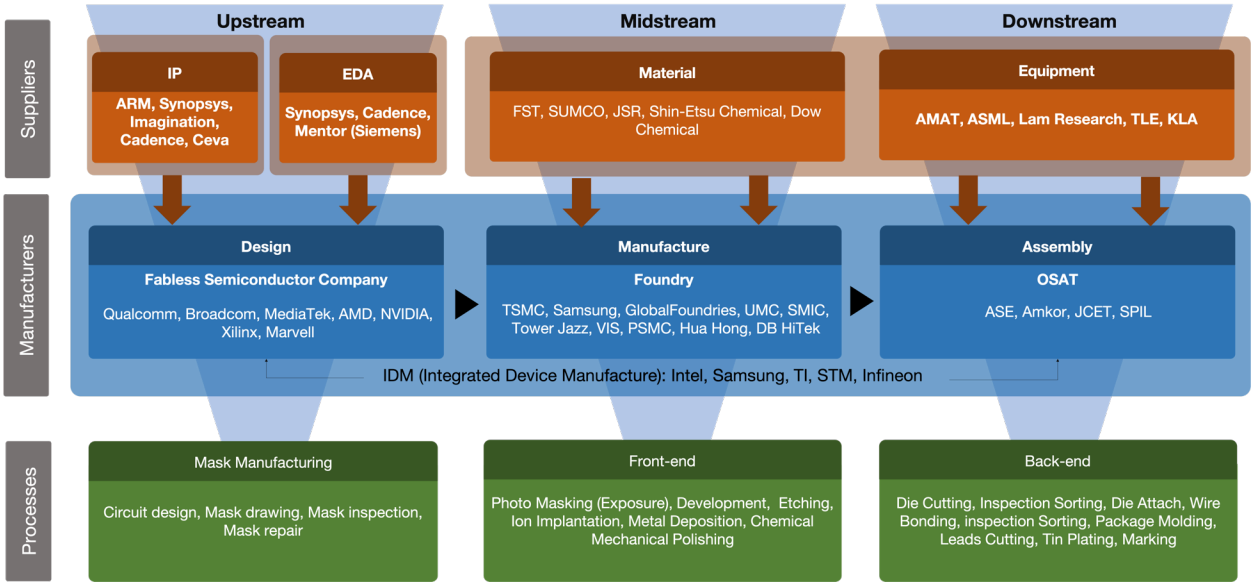
The iPhone 12's A14 bionic semiconductor chip has 11.8 billion transistors on it, a 38.8% increase from the previous A13's 8.5 billion.[4] It began its life in electric design automation (EDA) software operated by Apple's engineers. After those designs are transmitted to the foundry, the creation process of leading edge semiconductors takes over – arguably the most complex and difficult process ever accomplished by mankind, surpassing even the scientific accomplishment of getting to the moon. It is sensitive and difficult to control, and the foundries must be kept steady as they run day and night.




Pic - 1. Semiconductor Foundry Process Overview

[4] Omar Sohail, "Apple A14 Bionic Gets Highlighted With 11.8 Billion Transistors, 40% Higher Performance, New 6-Core CPU, and More", Wccf tech, Sept. 15 2020

The first major hurdle, photolithography, requires the creation of extreme ultraviolet light (EUV), which is created when molten tin is poured in a vacuum and hit with a laser roughly 50,000 times a second. It's the kind of thing that the real-life Tony Starks of our world are working on right now. This process must then be sustained so that the EUV can be bounced off of specially prepared mirrors to where it can be used to inscribe lines on microchips that are, in leading edge chips, an average of 15 atoms apart.[5] An intruder in the system, or one successfully executed piece of malware, is all it takes to severely disrupt the operation or just lock it up indefinitely, requiring a time-intensive system restore. State-sponsored and private malicious actors alike have many reasons to roll the dice and test the defenses of crucial players in the semiconductor supply chain.




Pic - 2. Semiconductor Industry Eco-System Overview

The semiconductor supply chain has more single, vital links than perhaps any industry in the world, where only one company can carry the product to the next step. Every link in the backbone of this industry must be sequentially reinforced and protected. A compromised system anywhere in the chain foreshadows a crisis, and an attack on any organization in the semiconductor industry is an attack on all of them. As cyber attacks

[5] Jon Bathgate, Brinton Johns, Shane Parrish, "All about SEMICONDUCTORS", The Knowledge Project, Nov. 23 2020

only become more and more frequent and advanced with every passing year, they also become more sophisticated and more able to specifically target work sites using industry-specific knowledge.

In 2018, the 'Chimera' threat group emerged, specifically targeting the semiconductor industry. Meanwhile, the COVID-19 pandemic has caused attack surfaces to rapidly expand, giving bad actors many more potential springboards on which to start an attack.[6] As a direct result of COVID-19, "From February to April 2020, the use of software for remote diagnosis among chipmakers more than doubled[.]"[7] Coincidentally, semiconductors were vital in mapping COVID-19's genome in less than 40 hours.[8]

A large foundry easily has thousands of individual devices for the fab process from 100 or more different vendors, and one asset could be linked with multiple computers, all running different operating systems, while as many as 30 different operating system types may exist in fabs.[9] These thousands of devices are connected to a network that a rogue piece of malware can hop around just as easily as an approved technician can if the correct safeguards are not in place. In this uniquely sensitive process, tampering or interference with any one of these numerous devices could easily be used to cause shutdown or havoc. The solution that is applied to protect these systems must therefore be transparent and able to coexist smoothly with every asset, operating system, and protocol used in the operating environment.

---

[6] The MITRE Corporation, "Chimera, Group G0114", Oct. 05 2020

[7] Mark Lapedus, "Industry Pushes For Fab Tool Security Standards", Sept. 17 2020

[8] Charlie Campbell, "Exclusive: The Chinese Scientist Who Sequenced the First COVID-19 Genome Speaks Out About the Controversies Surrounding His Work", Aug. 24 2020

[9] ibid.

# The Unique Needs of the Wafer Fab

How does an attack reach a foundry? Often by no fault of the organization, for example when a vendor comes by to install software on assets without first running an antivirus scan. Such an infection rapidly spreads across the company's network, even from city to city. Even a routine process that has happened tens of thousands of times without a hitch can become an attack vector able to take anybody by surprise. Leaders in the semiconductor industry have gone on to design and implement a rigorous cyber security posture, weathering the storm with stoicism and grace and building a bastion of resilient defenses to safeguard their future work.

Due to the fast, regular, and critically necessary turnaround in semiconductors, all security appliances must have zero impact on operations. Wafer fab frontrunners base their cyber security posture, like their production, on the principle of automating as much as possible. This eliminates the potential for human error and streamlines the operation. However, when automation is in use a factory's cyber defenses must be maintained to a higher standard. The key pain point is the complexity of the wafer fab process, which is so complex that most companies – even those that were once industry visionaries – have given up on doing it themselves and started outsourcing. Every part of the operational cycle must be conditioned to keep the operation running no matter what happens.

# SEMI: The Fast-Approaching New Standards

Semiconductor production has very little margin for error or variation. In the future, the standards of securing factories will only be more and more formalized. SEMI standards 6506, 6565, and 6566 are currently in development with the guidance of Intel, Cimetrix, TSMC, and the Industrial Technology Research Institute.[10] The new standards are expected to arrive in September, putting in place regulations that will sharply define security procedures for the industry.

At first this will be a hurdle, but in the long run it will be what protects the world from the results of damage to this critical industry – an ounce of prevention is worth a pound of cure. This collective effort minimizes risk and upgrades cyber defense by creating clear, unified expectations for the entire value stack. Industry giants will need to find solutions tailored to these regulations, which can be expected to place special emphasis on computing system security of fab equipment.

[10] Mark Lapedus, "Industry Pushes For Fab Tool Security Standards", Sept. 17 2020

# The 4 Cornerstones of an Operationally Resilient Security Appliance for Wafer Fabrication

1. An all-in-one box for policy deployment and high availability
2. Centralized cyber defenses offer high security with minimized cost
3. Protocol-sensitive virtual patching to safeguard sensitive legacy assets
4. Access to world-class security intelligence

## 1. An all-in-one box for policy deployment and high availability

Between every production tool and the switch there needs to be a security appliance, and that line between the tool and the switch must be both failsafe and able to provide unique policies to each production tool. This individual capability can come from an IPS unit hooked up to each device. But in a foundry this would require thousands of IPS units – the solution needs to be as aggregated as possible while still having individual capability for every tool on a line-by-line, tool-by-tool basis.

Furthermore, should the security appliance fail, the line between the production tool and the switch must remain functional to keep the operation running. This way, during troubleshooting the device can be quickly checked off as a potential point of failure, making it easier to narrow down the cause of any issue. It also means that when the appliance is being maintained, for example given pattern and signature updates, the line stays open so the tool can continue to operate. Fail safety streamlines the recovery process in conditions of hardware failure. An ideal security appliance will also have a redundant power supply – all this in one box.

## 2. Centralized cyber defenses offer high security with minimized cost

The ideal solution must reduce tasks, allow low support costs, and allow the IT department to do their job interference in the operation of pioneer production tools. Leaders in wafer fab prioritize productivity at the same time as cybersecurity by running cyber defense appliances that add little or no latency. These appliances should centralize threat responses as much as possible.

Solutions created with less complex industries and loadouts in mind are totally incapable of serving the needs of a foundry! To keep the operation running, and to make it feasible for security intelligence specialists to track and maintain the security

of all assets, a solution must be acquired that was purpose-built for these scenarios, and which includes direct communication with industry leaders who are developing the technology and doing the work.

## 3. Protocol-sensitive virtual patching to safeguard sensitive legacy assets

According to SEMI, more than 20 relevant operating systems went end-of-service from 1995 to 2018, and we can expect that every year 1 to 2 versions of utilized OSes will become End of Service (EOS) per year.[11] With every production tool having a life cycle of 20 years and OSes inevitably passing their end-of-service date, foundries are likely to have a large number of legacy systems requiring special protection. With the multitude of legacy assets operating in any foundry, part of the groundwork for preventing disruption is finding a solution that is custom-fit to assets running well past their end-of-service date. These legacy assets must be protected by resilient solutions that are immediately updated whenever a new type of threat is discovered.

Virtual patch technology is network-based so that it requires no installation or changes to assets. It should be provided by a security appliance deployed immediately after the switch. This technology requires the support of a dedicated team of threat specialists that provides up-to-date threat patterns and signatures in updates as well as communicating or working together with the foundry's own security team when necessary.

## 4. Access to world-class security intelligence

Security intelligence provided to work sites to support the efforts of their security operations center (SOC) can only keep up with the efforts of modern hackers if they

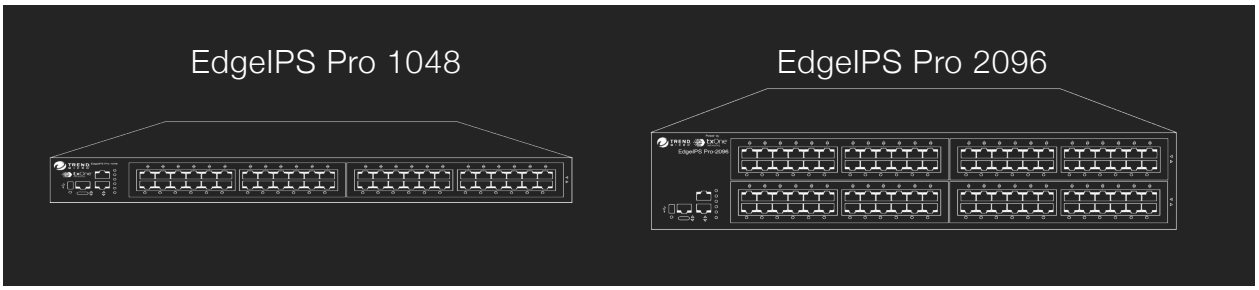
[11] SEMI, "Background Statement for SEMI Draft Document 6506 'New Standard: Specification for Cybersecurity of Fab Equipment'", accessed Feb. 25 2021

have round-the-clock support from dedicated specialists. Inline cybersecurity solutions must be more than just a piece of hardware – the solution must be able to adapt to changes in the threat landscape, as well as able to be maintained in concert with a leading edge knowledge base. A quick response should be expected and necessary, as well as the patience and capacity for high-urgency turnaround.

# EdgeIPS Pro, The Purpose-Built Solution for Wafer Fabs

EdgeIPS Pro was specifically designed with these cornerstones in mind, especially the upcoming new SEMI standards. It is the first of its kind: a centralized, resilient defense system with a straightforward and humanized interface. This rack-mounted IPS array, an aggregated set of 24 or 48 ports paired to provide hardware redundancy, deploys in the clean room's 1U server rack right under the core switch to reduce tasks and streamline defenses. In our deployments, we have found that the 24-pair model is the best fit for wafer fabs due to its compact size.

Since the EdgeIPS Pro is essentially 24 intrusion prevention systems integrated together, production assets are able to be managed and monitored from a single location while each set is also provided with its own unique policy. Each redundant pair is essentially its own network segment, able to be given independent policy while deep packet inspection is applied to all traffic. Total configurability such as this prevents interference with operations. This is one device that can monitor a vast number of production assets.



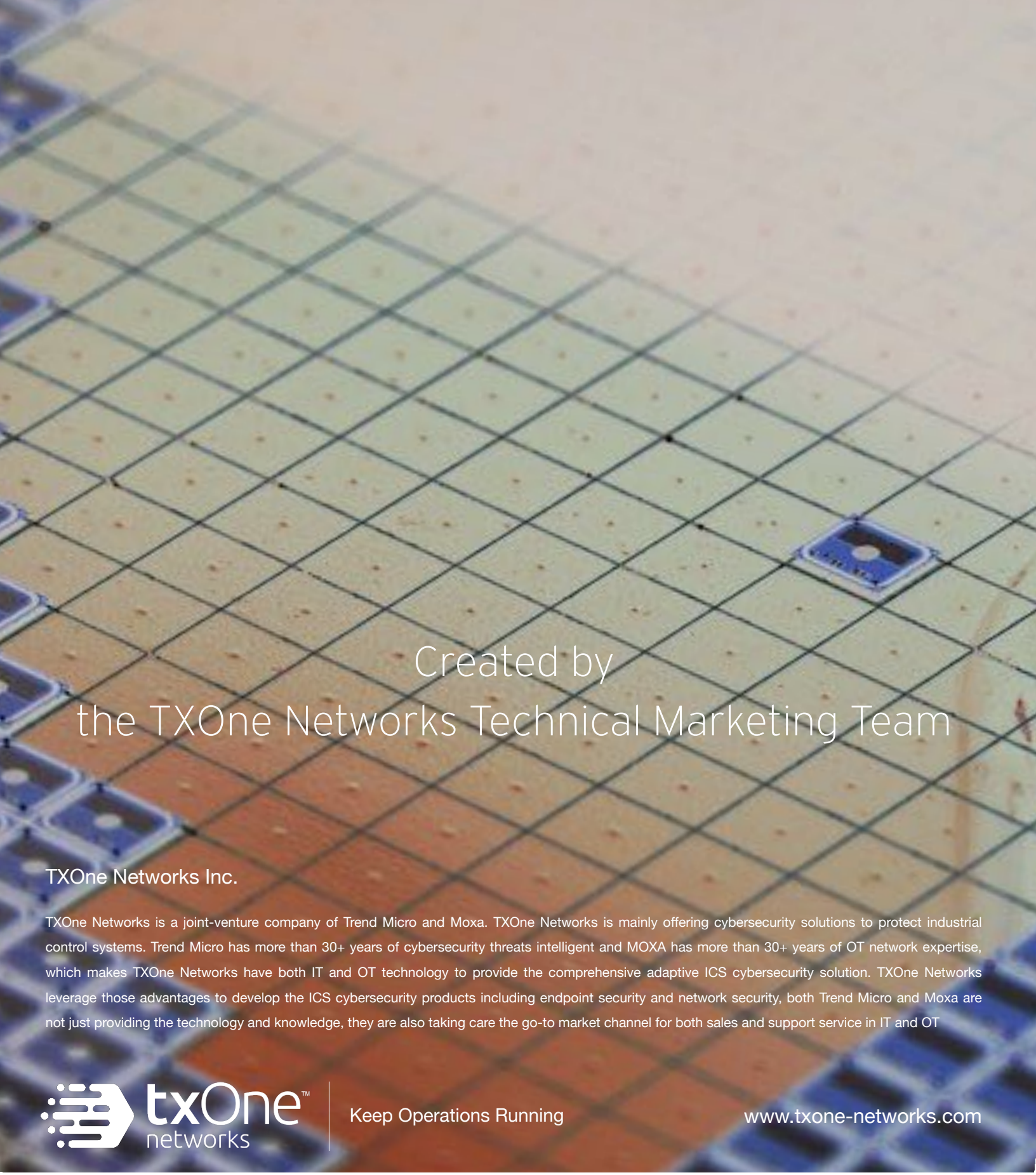

Many of the assets in a foundry environment are likely to be running different legacy systems. EdgeIPS Pro covers the vulnerabilities of every legacy system that could show up in an operating environment without any need to run any kind of installation on or modify the asset. Virtual patch makes a network-based "shield bubble" around

the device instead, ensuring the validity and security of traffic going in and out of the device while alerting the SOC to any abnormality.

EdgeIPS Pro's humanized interface design and integration with our OT Defense Console (ODC) eliminates alert fatigue and makes securing a vast collection of devices and assets significantly easier. ODC operates as one centralized management console to manage every EdgeIPS Pro deployed in a factory. This is a first-of-its-kind appliance designed specifically for organizations with their own trained team of security intelligence experts, empowering them with improved visibility and higher security awareness at a vastly reduced maintenance cost, specially designed for security intelligence experts working in the most sensitive operational environment in the world.

EdgeIPS Pro is supported by an instant response level of service, with quick turnaround on reporting and confirmation when we receive threat reports - so stakeholders can learn if it's a false positive or a false negative as quickly as possible. Our technology is designed to interface with your own experts and our threat specialists are experienced in collaboration with their on-site counterparts, be it your privately-run security team or an outsourced security team. For organizations running outsourced security systems, EdgeIPS Pro enables managed security service providers (MSSPs) to deliver dexterous, reliable OT security and network services.

Every wafer fab network is segmented on a larger scale that most work sites don't need to imagine. In a rising number of factories, thousands of production tools are already maintained and protected with the deployment of EdgeIPS Pro appliances managed on a large scale via ODC. Only an appliance continuously developed collaboratively with this kind of engagement from industry leaders has the ability to serve an environment on this grand scale.



# Created by
# the TXOne Networks Technical Marketing Team

## TXOne Networks Inc.

TXOne Networks is a joint-venture company of Trend Micro and Moxa. TXOne Networks is mainly offering cybersecurity solutions to protect industrial control systems. Trend Micro has more than 30+ years of cybersecurity threats intelligent and MOXA has more than 30+ years of OT network expertise, which makes TXOne Networks have both IT and OT technology to provide the comprehensive adaptive ICS cybersecurity solution. TXOne Networks leverage those advantages to develop the ICS cybersecurity products including endpoint security and network security, both Trend Micro and Moxa are not just providing the technology and knowledge, they are also taking care the go-to market channel for both sales and support service in IT and OT

txOne networks | Keep Operations Running

www.txone-networks.com