

# Kaspersky OT CyberSecurity:

Safeguarding semiconductors, chips, batteries and solar production across the world's most complex industrial environments



kaspersky

# Cybersecurity For High-Tech Electronics

Cybersecurity is critical in the semiconductor industry to safeguard intellectual property, sensitive designs and manufacturing processes against cyberthreats that can cause financial losses and erode competitive advantage. Securing this infrastructure also helps prevent global supply chain disruptions and ensures the integrity of devices across multiple industries.

## How OT security differs from IT

It's not realistic to apply IT cybersecurity best practices to the operational technology (OT) side of your organization. IT and OT environments involve fundamentally different devices and network structures:

- IT security focuses on digital data while ICS and OT focus on physical processes and safety
- Traditional IT security tools are not designed for OT threats or vulnerabilities
- That makes using them in OT networks can lead to unpredictable behavior and even devastating consequences
- Nevertheless, OT systems are being integrated with IT thus unified security approach is crucial

## Industry Shifts in High-Tech Manufacturing



### Industry 4.0

Global chip shortages have accelerated the adoption of Industry 4.0. Manufacturers are introducing IoT-enabled equipment and AI-driven automation to maximize production efficiency and scalability



### Smart Fabs

The rise of smart fabs is transforming the industry, integrating OT and IT systems, applying predictive maintenance and using digital twins to drive continuous operational improvement



### Supply chain fragmentation

High-tech manufacturing increasingly depends on outsourced production stages and specialized third-party tooling. This diversifies capabilities but makes ecosystems more complex



### Digital twins & AI/ML

Digital twins and machine-learning models are increasingly being used to simulate and optimize production processes in real time. TSMC's "Smart Fabs," for example, apply AI/ML and digital twin technology to continuously improve efficiency



### Private networks in fabs

Major fabs are deploying dedicated private networks, such as Samsung's Texas plant with private 5G, to ensure fast, reliable and secure industrial connectivity



### Device restrictions

To protect sensitive processes and intellectual property, many fabs prohibit mobile devices and USB drives in production areas

# Top Attack Vectors And Real Incidents

High-tech fabs face escalating cyberthreats due to their complexity. Attackers actively exploit known vectors.

## Observed Vulnerabilities

### Legacy OT systems

80% of semiconductor equipment still runs on Windows 7/XP. Many such systems from the 1990s cannot be patched

### Compromised third-party access

Global supply chains give external individuals – vendors, contractors, etc. – access to sensitive data

### Nation-State attacks

Campaigns designed to disrupt, spy on or steal data from other countries, corporations or critical infrastructure

### Single points of failure

EUV machines depend on 500k+ components. A single compromise in firmware could impact the whole production

### Insider threats

Employees or contractors may steal IP, sabotage systems or unintentionally compromise security through human error

## 2018

### TSMC – WannaCry attack

RANSOMWARE

Vector: Unpatched infection in Windows  
Impact: Shutdown of multiple chip fabrication plants and production delays, ~ \$256M revenue hit

## 2022

### IP theft on Taiwanese chipmaker

ESPIONAGE

Vector: A vendor's compromised VPN resulted in a MES system breach for the chipmaker  
Impact: Stolen 5nm designs sold to competitors

## 2024

### AMD data leak

ESPIONAGE

Vector: Leak of internal communications and data  
Impact: Data offered for sale on the dark web

### Intra attack on microchip technology

SABOTAGE

Vector: Disrupted servers and business operations  
Impact: Forced shutdown of affected systems

## 2021

### SolarWinds-style attack

SUPPLY CHAIN ATTACK

Vector: Compromised vendor software  
Impact: 200+ tools infected with backdoors (undetected for 9 months)

## 2023

### Phishing attack on Korean fab

RANSOMWARE

Vector: Phishing attack resulted in lateral movement within the victim's OT network  
Impact: 3-day shutdown, \$70M financial loss

### TSMC data breach

SUPPLY CHAIN ATTACK

Vector: Cyberattack on a third-party supplier  
Impact: \$70 million ransom demand

### Applied Materials Inc sabotage

SABOTAGE

Vector: Undisclosed cyberattack on supplier MKS  
Impact: Supply disruption and revenue shortfall

\* not audited or confirmed by organizations

# SEMI: Industry Cybersecurity Standards

To combat emerging threats, SEMI is driving the development and ongoing refinement of cybersecurity standards to safeguard the semiconductor and electronics industry. Two key standards have been introduced:



## E187: Cybersecurity for new equipment

focuses on security requirements during the development phase, before equipment is commissioned.

Applies to computing devices in new equipment running Microsoft Windows or Linux.



## E188: Cybersecurity for existing equipment

focuses on safe operating procedures to eliminate malware from already commissioned equipment.

Applies to any computing device in existing equipment, including computers, controllers and PLCs.

## Complementarity of SEMI standards

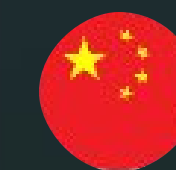
Integration of SEMI E187 and SEMI E188 establishes a comprehensive framework for defending the semiconductor industry against cybersecurity threats. It's crucial to implement OT-aware cybersecurity controls, including:

- Network segmentation
- Endpoint protection
- Vulnerability scanning
- Network security and traffic monitoring
- Access control
- System hardening
- OS security (patching, updates, hardening)
- Security monitoring (log management and configuration change tracking)

## Global regulatory pressures

Governments worldwide are enforcing strict cybersecurity regulations to protect critical infrastructure and high-tech supply chains.

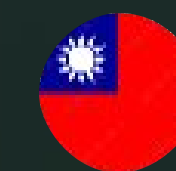
### Key Regulations



**CHINA:**  
MLPS 2.0 + Data Security Law



**USA:**  
NIST SP 800-82, CISA Critical Infrastructure Guidelines



**TAIWAN:**  
Cybersecurity Management Act



**EU:**  
NIS2, Cyber Resilience Act (2025)



**SOUTH KOREA:**  
K-Semiconductor Strategy (2021)

# Vendor-Driven Initiatives In Semiconductor Cybersecurity

## TSMC

invests around \$300 million annually in cybersecurity. Initiatives include digital deception, where fake process data is used to mislead attackers, and Cyber Shield an AI-driven anomaly detection system for OT networks

## KLA

applies zero-trust frameworks to remote equipment monitoring, verifying every access request and continuously monitoring activity

## INTEL, SAMSUNG

integrate SIL-4 certified safety systems into process control, ensuring maximum operational reliability. They also apply Faraday Zone isolation concepts in advanced R&D facilities, such as 3nm development, to limit exposure of sensitive asset.

\* not audited or confirmed by organizations

Even semiconductor giants with robust internal cybersecurity measures rely on third-party solutions for several strategic reasons:

- Specialized solutions address threats unique to OT
- Legacy support is required to support many older systems that cannot run modern in-house security tools
- Sector and legislative standards require vendor-validated security tools for compliance
- Cybersecurity firms aggregate data from multiple fabs, identifying trends and strengthening protection
- Developing ICS-aware tools such as XDR in-house could take 5+ years and (\$50M+)
- Specialist third parties discover vulnerabilities internal teams may miss

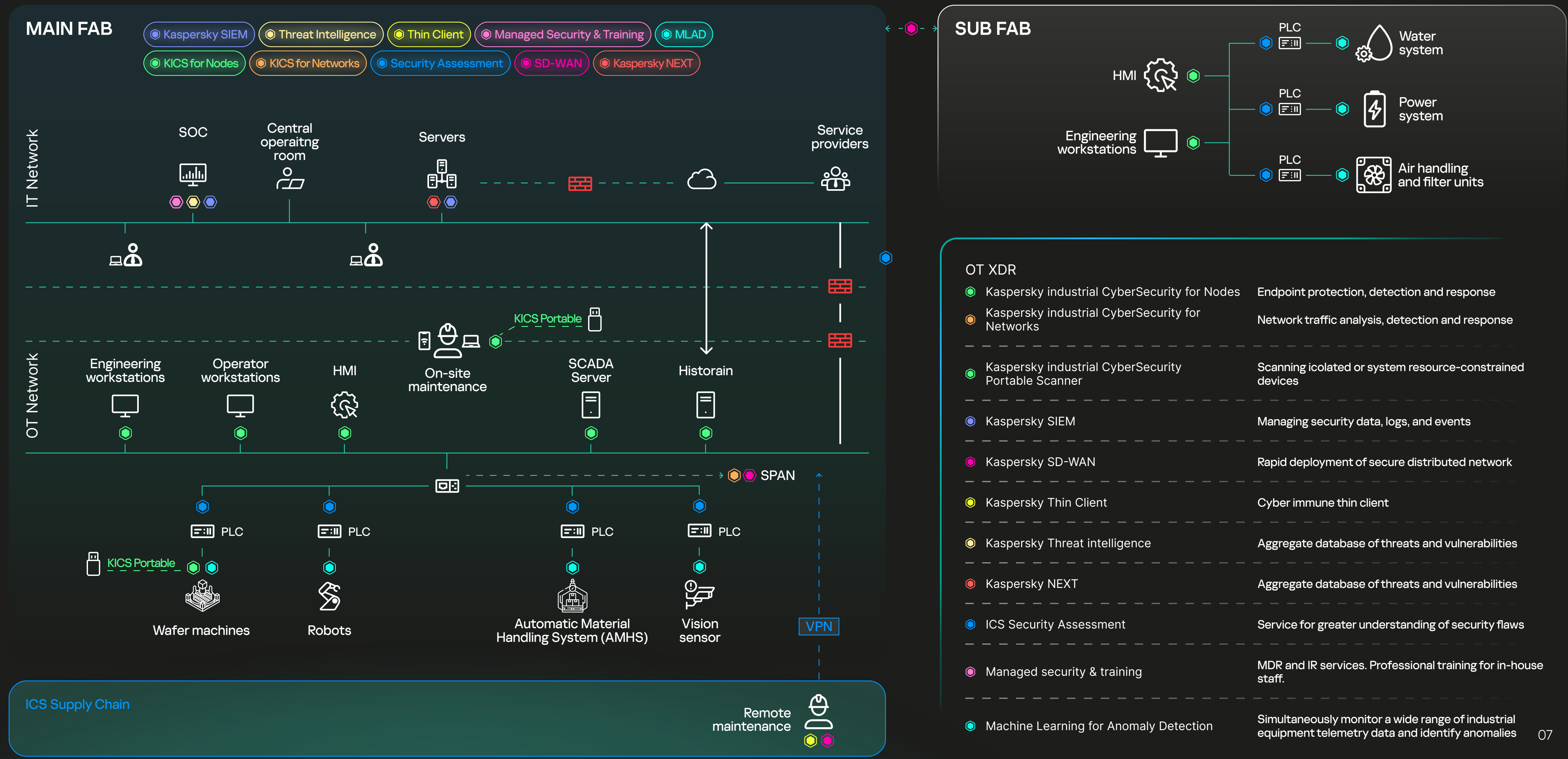
No single organization can address every cyberthreat on its own. Regulatory and customer demands increasingly favor certified solutions, while the complexity and legacy burden of OT environments make external expertise essential.

# Addressing key OT challenges with Kaspersky CyberSecurity







In the high-tech industry, every incident can cost millions, disrupt global supply chains and undermine hard-earned trust. The Kaspersky OT CyberSecurity helps manufacturers stay ahead of these risks, enabling resilient production, compliance with global standards, and secure innovation across even the most complex and legacy-heavy environments.

	SEMI baseline cybersecurity requirements	Sub-tasks	Kaspersky capabilities	Kaspersky offering
<b>Network security</b> <b>Endpoint protection</b> <b>Vulnerability scanning</b> <b>System hardening</b> <b>OS security</b> (patch / update / hardening)	●		<b>OT XDR platform</b> * Network Traffic Analysis (NTA), detection and response * Endpoint Protection, Detection and Response software  <b>Advanced assets management</b> * Vulnerability scan * Compliance audit * Configuration change monitoring	 Kaspersky Industrial CyberSecurity
<b>Access Control</b>	●		<b>Secure access to infrastructure</b> * Rapid deployment of reliable geographically distributed OT networks for critical data acquisition * Secure connection to OT infrastructure through cyber-immune clients	 Kaspersky Thin Client   Kaspersky SD-WAN
<b>Security monitoring</b> (logs and configuration changes management)	●		<b>Log management with data sovereignty</b>	 Kaspersky Unified Monitoring and Analysis Platform
<b>Secure development lifecycle</b>	●		* Compliance with IEC 62443-4-1 * Product Cybersecurity Assessment	 Kaspersky ICS Security Assessment
<b>Legacy systems coverage</b>	●	●	* Support for Win starts from XP SP2+ and 30+ Linux versions * Security updates even for air-gapped * Air-gapped machines scanning	 Kaspersky Industrial CyberSecurity
<b>Bridging the workforce gap</b>	●	●	<b>Training &amp; consulting</b> <b>Managed security</b>	 Kaspersky Managed Detection and Response  Kaspersky Automated Security Awareness Platform  Dedicated Technical Account Manager
<b>OT resilience</b>	●	●	<b>200+ compatibility certificates</b> <b>Non-intrusive settings, no reboot installation &amp; updates</b> <b>Tunable resource consumption</b>	 Kaspersky Industrial CyberSecurity
<b>Build own OT or IT-OT SOC</b>	●	●	IT-OT convergence, centralized monitoring SOC consulting	 Kaspersky Professional Services  Kaspersky Threat Intelligence   Kaspersky OT CyberSecurity
<b>Predictive maintenance of mission-critical assets</b>	●	●	Anomaly detection for industrial assets	 Kaspersky Machine Learning for Anomaly Detection (MLAD)
<b>Streamlined, cost-effective solution</b>	●	●	Seamless integration Single-vendor support Faster incident response	 Kaspersky OT CyberSecurity

# Kaspersky OT CyberSecurity: Product application points



# Cyber Resilience with the Kaspersky OT CyberSecurity

 <p><b>Inventory and assess</b></p> <p>Expertise</p>	 <p><b>Essential security</b></p> <p>Technology</p>	 <p><b>Advanced threat detection, audits and compliance</b></p> <p>Knowledge+Technology+Expertise</p>	 <p><b>Network segmentation</b></p> <p>Knowledge+Technology+Expertise</p>	 <p><b>Mature security operations</b></p> <p>Knowledge+Technology+Expertise</p>	 <p><b>Fault tolerance and readiness</b></p> <p>Technology</p>
<p><b>Network Asset Discovery</b></p> <ul style="list-style-type: none"> <li>Identify all hardware and software assets within the OT infrastructure</li> <li>Create a detailed inventory to plan your cybersecurity strategy</li> </ul> <p><b>Endpoint Inventory</b></p> <ul style="list-style-type: none"> <li>Catalog hardware and software components</li> <li>Identify critical assets and vulnerabilities with an up-to-date inventory</li> </ul> <p><b>Policy Development</b></p> <ul style="list-style-type: none"> <li>Develop comprehensive policies and procedures</li> <li>Establish cybersecurity levels and identify required controls with hazard and impact analysis</li> </ul>	<p><b>OS Hardening</b></p> <ul style="list-style-type: none"> <li>Configure systems securely; apply patches and updates regularly</li> <li>Implement additional controls</li> <li>Prevent exploits and check removable devices Application Control</li> </ul> <p><b>Application Control</b></p> <ul style="list-style-type: none"> <li>Maintain system integrity by restricting unauthorized applications</li> </ul> <p><b>Endpoint Protection</b></p> <ul style="list-style-type: none"> <li>Implement anti-malware to protect devices across ICS and OT environments</li> </ul>	<p><b>Network Visibility</b></p> <ul style="list-style-type: none"> <li>Monitor network traffic to detect anomalies and understand attack patterns</li> </ul> <p><b>Threat and Anomaly Detection</b></p> <ul style="list-style-type: none"> <li>Use machine learning and DPI to identify network intrusions and anomalies</li> <li>Use EDR technology to monitor OT host telemetry</li> </ul> <p><b>Security Audits</b></p> <ul style="list-style-type: none"> <li>Conduct regular vulnerability scans and compliance audits</li> <li>Maintain detailed system audits and control configurations</li> </ul> <p><b>Compliance Management</b></p> <ul style="list-style-type: none"> <li>Ensure compliance with regulatory requirements and industry standards</li> </ul>	<p><b>Intrusion Prevention</b></p> <ul style="list-style-type: none"> <li>Boost threat detection and prevention through integration with existing network infrastructure</li> </ul> <p><b>Restricted Data Flow</b></p> <ul style="list-style-type: none"> <li>Optimize segmentation and data flow with SD-WAN and VLANs</li> <li>Enforce security controls even in remote or smaller locations</li> </ul> <p><b>IoT Controls</b></p> <ul style="list-style-type: none"> <li>Implement security controls visibility with advanced secure-by-design gateways and protocols for IoT devices</li> </ul> <p><b>Remote Access</b></p> <ul style="list-style-type: none"> <li>Control remote access with thin clients and secure gateways</li> </ul>	<p><b>Industrial SOC Threat Intelligence</b></p> <ul style="list-style-type: none"> <li>Leverage real-time threat intelligence to protect against malware, phishing, vulnerabilities and exploits</li> </ul> <p><b>SOC Consulting</b></p> <ul style="list-style-type: none"> <li>Engage experts to strengthen your SOC's ability to handle sophisticated threats</li> </ul> <p><b>Converged IT-OT Detection and Response</b></p> <ul style="list-style-type: none"> <li>Integrate IT and OT security for unified threat detection and response</li> </ul> <p><b>Managed Protection</b></p> <ul style="list-style-type: none"> <li>Rely on managed detection and response services for continuous monitoring and expert incident handling</li> </ul>	<p><b>Expert Training</b></p> <ul style="list-style-type: none"> <li>Provide specialized cybersecurity training for staff to handle and mitigate incidents effectively</li> </ul> <p><b>Awareness Training</b></p> <ul style="list-style-type: none"> <li>Conduct regular training sessions to increase organization-wide awareness and readiness</li> </ul> <p><b>Asset Performance Analysis</b></p> <ul style="list-style-type: none"> <li>Apply tools and methodologies to analyze asset performance, ensure reliability and detect potential failures</li> </ul>

Learn more about Kaspersky's comprehensive cybersecurity approach.



# Kaspersky's High Tech Track Record

Kaspersky brings over a decade of leadership in detecting and analyzing advanced persistent threats — including those targeting critical infrastructure and industrial systems— supported by global threat intelligence, trusted to protect over a billion devices, and a proven track record of real-world impact



## Robust cybersecurity

measures compliant with multiple regulatory standards



## Supports legacy and contemporary systems,

ensuring that all components of the ICS are protected



## 200+ compatibility certificates

from 70+ vendors



## Non-intrusive settings

and modular deployment



## Integration

of corporate and industrial environments into a unified, secure infrastructure with end-to-end security

# 50 000+

licenses shipped

to electronic component manufacturers

# 20+

projects completed

in semiconductor, battery and LCD/OLED display industries

## Success stories from the high-tech industry

### Pioneer in lithium-ion batteries

We protect gigafactories in China and Europe for a global leader in high-performance, sustainable energy storage for electric vehicles and renewable energy systems.

### Key EV battery partner

We secure the production lines of a major supplier to electric vehicle giants and energy storage providers that control a significant share of the world's lithium-battery market.

### Multinational OEM electronics manufacturer

We deliver cybersecurity for one of the world's largest electronics contract manufacturers, with annual revenues exceeding \$150B.

### Global smart terminal display leader

We protect a global leader whose displays are built into a quarter of the world's smart terminals. The company operates multiple large-scale manufacturing sites and subsidiaries across 20 countries and regions.

# Stronger together: Partner with Kaspersky for end-to-end cyber protection

The Kaspersky OT CyberSecurity covers everything from legacy system risks and supply chain vulnerabilities to regulatory pressures. Field-proven in the most complex industrial environments, it protects some of the world's largest fabs and helps keep them ahead of modern threats. Let's talk about how we can secure yours



Kaspersky  
OT CyberSecurity



Kaspersky  
Industrial  
CyberSecurity

[www.kaspersky.com](http://www.kaspersky.com)

© 2025 AO Kaspersky Lab.  
Registered trademarks and service marks  
are the property of their respective owners.

Manage your security with Kaspersky  
and become a partner

Contact us and take part in our global customer conference

[Learn more](#)

#kaspersky  
#bringonthefuture