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

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

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

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

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

2018

TSMC – WannaCry attack RANSOMWARE

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

2021

SolarWinds-style attack SUPPLY CHAIN ATTACK

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

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

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

Applied Materials Inc sabotage SABOTAGE

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

TSMC data breach SUPPLY CHAIN ATTACK

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

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

* 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

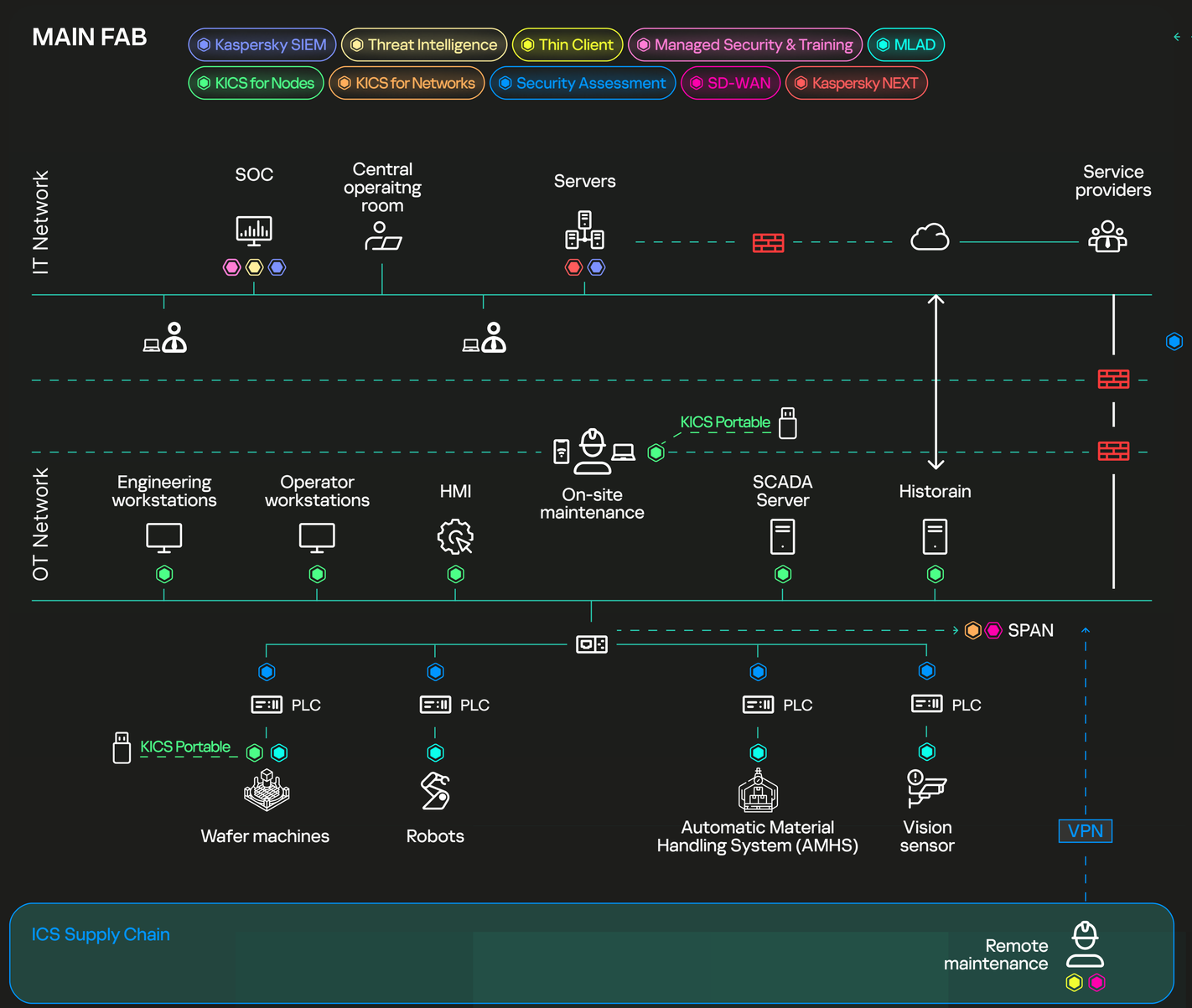
No single organization can address every cyberthreat on its own. Regulatory and customer demands increasingly favor certified solutions, while the complexity and legacy burden of OT environments make external expertise essential.

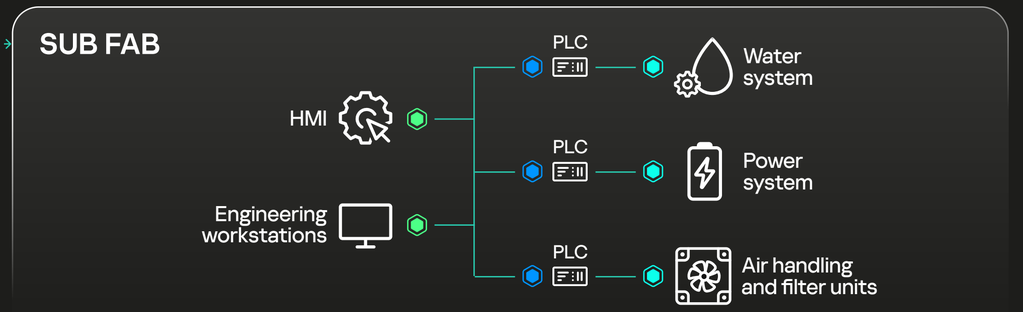
Addressing key OT challenges with Kaspersky CyberSecurity

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
Network security **Endpoint protection** **Vulnerability scanning** **System hardening** **OS security** (patch / update / hardening)	⬢		**OT XDR platform** * Network Traffic Analysis (NTA), detection and response * Endpoint Protection, Detection and Response software **Advanced assets management** * Vulnerability scan * Compliance audit * Configuration change monitoring	
Access Control	⬢		**Secure access to infrastructure** * Rapid deployment of reliable geographically distributed OT networks for critical data acquisition * Secure connection to OT infrastructure through cyber-immune clients	
Security monitoring (logs and configuration changes management)	⬢		**Log management with data sovereignty**	
Secure development lifecycle	⬢		* Compliance with IEC 62443-4-1 * Product Cybersecurity Assessment	
Legacy systems coverage		⬢	* Support for Win starts from XP SP2+ and 30+ Linux versions * Security updates even for air-gapped * Air-gapped machines scanning	
Bridging the workforce gap		⬢	**Training & consulting** **Managed security**	
OT resilience		⬢	**200+ compatibility certificates** **Non-intrusive settings, no reboot installation & updates** **Tunable resource consumption**	
Build own OT or IT-OT SOC		⬢	**IT-OT convergence, centralized monitoring** **SOC consulting**	
Predictive maintenance of mission-critical assets		⬢	**Anomaly detection for industrial assets**	
Streamlined, cost-effective solution		⬢	**Seamless integration** **Single-vendor support** **Faster incident response**	

Kaspersky OT CyberSecurity: Product application points





OT XDR

Kaspersky industrial CyberSecurity for Nodes	Endpoint protection, detection and response
Kaspersky industrial CyberSecurity for Networks	Network traffic analysis, detection and response
Kaspersky industrial CyberSecurity Portable Scanner	Scanning icolated or system resource-constrained devices
Kaspersky SIEM	Managing security data, logs, and events
Kaspersky SD-WAN	Rapid deployment of secure distributed network
Kaspersky Thin Client	Cyber immune thin client
Kaspersky Threat intelligence	Aggregate database of threats and vulnerabilities
Kaspersky NEXT	Aggregate database of threats and vulnerabilities
ICS Security Assessment	Service for greater understanding of security flaws
Managed security & training	MDR and IR services. Professional training for in-house staff.
Machine Learning for Anomaly Detection	Simultaneously monitor a wide range of industrial equipment telemetry data and identify anomalies

Cyber Resilience with the Kaspersky OT CyberSecurity

Inventory and assess

Expertise

Network Asset Discovery

- Identify all hardware and software assets within the OT infrastructure
- Create a detailed inventory to plan your cybersecurity strategy

Endpoint Inventory

- Catalog hardware and software components
- Identify critical assets and vulnerabilities with an up-to-date inventory

Policy Development

- Develop comprehensive policies and procedures
- Establish cybersecurity levels and identify required controls with hazard and impact analysis

Essential security

Technology

OS Hardening

- Configure systems securely; apply patches and updates regularly
- Implement additional controls
- Prevent exploits and check removable devices Application Control

Application Control

- Maintain system integrity by restricting unauthorized applications

Endpoint Protection

- Implement anti-malware to protect devices across ICS and OT environments

Advanced threat detection, audits and compliance

Knowledge+Technology+Expertise

Network Visibility

- Monitor network traffic to detect anomalies and understand attack patterns

Threatand Anomaly Detection

- Use machine learning and DPI to identify network intrusions and anomalies
- Use EDR technology to monitor OT host telemetry

Security Audits

- Conduct regular vulnerability scans and compliance audits
- Maintain detailed system audits and control configurations

Compliance Management

- Ensure compliance with regulatory requirements and industry standards

Network segmentation

Knowledge+Technology+Expertise

Intrusion Prevention

- Boost threat detection and prevention through integration with existing network infrastructure

Restricted Data Flow

- Optimize segmentation and data flow with SD-WAN and VLANs
- Enforce security controls even in remote or smaller locations

IIoTControls

- Implement security controls visibility with advanced secure-by-design gateways and protocols for IoT devices

Remote Access

- Control remote access with thin clients and secure gateways

Mature security operations

Knowledge+Technology+Expertise

Industrial SOC Threat Intelligence

- Leverage real-time threat intelligence to protect against malware, phishing, vulnerabilities and exploits

SOC Consulting

- Engage experts to strengthen your SOC's ability to handle sophisticated threats

Converged IT-OT Detection and Response

- Integrate IT and OT security for unified threat detection and response

Managed Protection

- Rely on managed detection and response services for continuous monitoring and expert incident handling

Fault tolerance and readiness

Technology

Expert Training

- Provide specialized cybersecurity training for staff to handle and mitigate incidents effectively

Awareness Training

- Conduct regular training sessions to increase organization-wide awareness and readiness

Asset Performance Analysis

- Apply tools and methodologies to analyze asset performance, ensure reliability and detect potential failures

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

50 000+
licenses shipped
to electronic component manufacturers

20+
projects completed
in semiconductor, battery and LCD/OLED display industries

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

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

Manage your security with Kaspersky and become a partner

Contact us and take part in our global customer conference

Learn more

#kaspersky
#bringonthefuture