Security Solutions for Smart Factories

Keep operations running

Products Included in our solution

<table>
<thead>
<tr>
<th>Prevention</th>
<th>Detection</th>
<th>Persistence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trend Micro TippingPoint Threat Protection System™</td>
<td>Intrusion prevention system</td>
<td>Built-in agent security for IoT devices</td>
</tr>
<tr>
<td>Trend Micro IoT Security™</td>
<td>Trend Micro Deep Discovery™ Inspector</td>
<td>Threat visualization and early detection</td>
</tr>
<tr>
<td>Trend Micro Deep Security™</td>
<td>EdgeFire™</td>
<td>Unified server security</td>
</tr>
<tr>
<td>Trend Micro Safe Lock™ TXOne Edition</td>
<td>EdgeIPS™</td>
<td>System lockdown software</td>
</tr>
<tr>
<td>Trend Micro Portable Security™ 3</td>
<td>OT Defense Console™</td>
<td>Virus scan and clean-up tool without installation</td>
</tr>
</tbody>
</table>

Threat intelligence supporting our solutions

Research security risks to the manufacturing industry specific, which covers both IT and OT

Vulnerability discovery community operated by Trend Micro

1400+ vulnerabilities reported in 2018

https://www.trendmicro.com/smartfactories

Operational stoppage risks due to cyberattacks

- **Risk 1**: Stoppage of manufacturing system due to virus infection
- **Risk 2**: Equipment damage due to system malfunction
- **Risk 3**: Production of defective products due to malfunction of equipment

Cyber Threats
Vulnerabilities & Exploits
Targeted Attacks
AI & ML
IoT
OT / IoT
Cybercriminal Undergrounds
Future Threat Landscape

USA Headquarters: Trend Micro Incorporated, 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone: 1-888-977-4200 Email: us_info@trendmicro.com

Canada Headquarters: Trend Micro Canada Technologies Inc., 40 Hines Road, Suite 200 Ottawa, Ontario, Canada K2K 2M5
Phone: 1-866-684-7332 Email: CanadaChannelSales@trendmicro.com

© 2019 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, Trend Micro TippingPoint Threat Protection System™, Trend Micro Deep Discovery™ Inspector, Trend Micro Deep Security™, Trend Micro Safe Lock™ TXOne Edition, EdgeFire™, EdgeIPS™, Trend Micro Portable Security™ 3, OT Defense Console™, Trend Micro IoT Security™, and other names of products and services are either trademarks or registered trademarks of Trend Micro Incorporated. Other names of companies, products, or services mentioned may be trademarks or registered trademarks of their respective companies.
Convergence of IT and OT: Protecting interconnected systems to improve efficiency.

Smart factories aim to improve production efficiency by using industrial IoT (IIoT) technologies and integrating with business systems. However, its adoption expands the attack surface, which benefits cyber attackers and increases the risk of operation stoppages. This makes foresight-driven IIoT security essential to smart factories.

Security challenges faced by smart factories

- **Low visibility**
  - There may be cases where there is no appropriate visibility from a security perspective.
  - Therefore, if there is a vulnerable device, effective and timely patching cannot be applied.

- **Unpatched devices**
  - You may have to wait for a planned outage.
  - As a result, patches cannot be applied even if the device is known to be vulnerable.

- **Weak authentication**
  - There are devices that can be accessed without authentication.
  - If it is used, a malicious actor may be able to operate a critical device.

**Trend Micro security solutions for smart factories**

**“Fortification of manufacturing system” approach:**
Layer-by-layer protection using IT security and OT security

**Prevention**
- Stop cyberattacks from the IT environment to the OT environment
  - Perimeter defense to prevent cyberattacks designed to exploit vulnerabilities
  - Protection of various IoT devices such as IoT gateways used in industrial services

**Detection**
- Identify internal activities of cyberattack in the OT environment
  - Monitor network traffic from multiple perspectives
  - Receive early detection of suspicious movements
  - Detect anomalies on the servers

**Persistence**
- Defend industrial control devices
  - Prevent the spread of infection by network segmentation
  - Protect critical equipment at the network level from cyberattacks designed to exploit vulnerabilities
  - Prevent the execution of malware and unauthorized programs (Lockdown)
  - Scan and clean up malware in the devices where security software can not be installed
  - Visualize asset information of production devices and security events