



CASE STUDY

One of India's Largest Producers of Aluminium

Securing the operational technology
devices that control aluminium production.

The Aluminium Producer wishes to preserve its image as a reliable supplier of quality aluminium. K7 supports this goal by ensuring their manufacturing facilities are protected against cyberattacks.

Client Snapshot

- » 80 endpoints (for production)
- » Top Performer, PAT Cycle II
- » Provides aluminium for Indian missiles

The client is one of India's largest aluminium producers and a critical pillar supporting the nation's development, which makes it a target of cyberwarfare and attacks for monetary gain. Robust, unobtrusive cybersecurity ensures that operations are cybersafe and protective systems do not hinder production.

Cybersecurity for Operational Technology Devices Supports Uninterrupted Manufacturing

The Client's Requirements

- Cybersecurity that doesn't block their apps
- Isolation of production devices from the internet
- No hardware performance degradation
- Hardware monitoring
- Reports for monitoring
- Restrictions on applications
- Alert notifications
- Strengthen national security



The K7 Solution

K7 Endpoint Security for Operational Technology (K7 EPS OT) provides reliable cybersecurity for manufacturing units without introducing production bottlenecks.



Accurate Threat Identification

The client's IT team had tested other cybersecurity solutions that had often identified production control software (proprietary and off-the-shelf) as malware and acted against the executables, disrupting manufacturing. K7's team demonstrated that K7 EPS OT accurately identified genuine files as benign and acted only against threats. The client's team were delighted that K7 EPS OT did not generate false positives and would not disrupt production.

Intranet-based Centralised Update Distribution

The client's management wished to isolate their operational technology infrastructure from the internet, and stipulated that operational endpoints should not receive updates directly through the internet. K7's team configured K7 EPS OT's console to receive the updates through the internet and distribute the updates to operational endpoints through the factory intranet, satisfying the client's management.

Low Impact Protection

The client's engineers were concerned that cybersecurity solutions would impact the stability of the operational technology devices used to control production. K7 EPS OT utilises K7's international award-winning scan engine that is world-renowned for its efficiency and ranked **World #1** for protecting devices without impacting performance.

K7's team offered a staggered deployment of K7 EPS OT that proved infrastructure stability was not affected and reassured the client's engineers that manufacturing activities would not be impacted by cybersecurity.

Hardware Asset Management

Maintaining the hardware specifications of operational technology devices is critical to the smooth functioning of the client's production facilities. The client's IT team were pleased that K7 EPS OT allowed them to monitor hardware configuration and alerted them if hardware changes were detected.

Custom Reports

The client's team required reports in varying formats to analyse cybersecurity across their production environment. K7 EPS OT allows the generation of custom reports which enables them to scrutinise enterprise cybersecurity in formats that match their requirements.

Application Control

Shadow IT is a concern for all cyber defenders and the client's team were keen to ensure that unauthorised applications couldn't be installed on production endpoints. They were pleased that K7 EPS OT enables viewing installed applications and can block applications from running, accessing the network, or accessing the internet, as required by their cybersecurity policy.

Email Alerts

The client's security team emphasised the need for prompt response to cybersecurity events and required a solution that would alert them as soon as an event was detected. K7 EPS OT supports email notifications for security alerts, which perfectly suited their requirements.

Made in India Cybersecurity

The client's management were keen to ensure that national security was not compromised by the cybersecurity solution and data sovereignty is maintained. K7 was founded in and is managed from India and our cybersecurity solutions are 100% Made in India with all IP designed and developed in India, which ensures that the client's contribution to the defence of the nation is reinforced.



K7 Security's **Endpoint Security for Operational Technology** is designed to protect digital infrastructure in production plants without interfering with the functioning of resource-intensive industrial control applications. **Contact Us** to learn more about how K7 can help you secure your manufacturing facilities with powerful and unobtrusive cybersecurity.



Copyright © 2025 K7 Enterprise Security Private Limited, All Rights Reserved.

This work may not be sold, transferred, adapted, abridged, copied, or reproduced in whole or in part in any manner or form or any media without the express prior written consent of authorised personnel of K7 Enterprise Security Private Limited. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners.

www.k7cybersecurity.com