



CASE STUDY

Armis Helps PGP Glass Gain Full Situational Awareness of OT Devices to Safeguard IP



The Challenge

- Protect sensitive and valuable intellectual property (IP)
- Gain visibility and full situational awareness of all assets across operational technology (OT) systems and connected IT systems
- Extract data from OT devices running on legacy Microsoft Windows systems
- Integrate data feeds into AI and ML analytical models

The Solution

- Deployed Armis Centrix™ in three plants in India and Sri Lanka
- Integrated Armis Centrix™ with multiple other systems across network
- Fed data from Armis Centrix™ into energy optimization model
- Positioned for a future shift into a cloud-based security environment

The Results

- Increased visibility and security across network
- Averted IP exfiltration through visibility into device metadata
- Improved energy efficiency in manufacturing processes
- Reduced waste in manufacturing processes
- Enabled savings of USD\$2 million equivalent per year in costs

Industry: **Manufacturing**

Location: **Mumbai, India**

Size: **Approximately 2,500 employees**



Armis Centrix™ for
OT/IoT Security



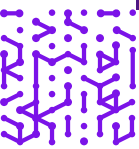
Armis Centrix™ for
VIPR - Prioritization and
Remediation

Background

PGP Glass, a Blackstone portfolio company, is a global leader in the design, decoration, and production of premium glass packaging solutions. With a footprint spanning India and Sri Lanka, and serving 17 of the top 20 global brands, their 12 furnaces and 65 production lines are dedicated to crafting exceptional glass that elevates brands worldwide.

The Challenge

PGP Glass holds a treasure trove of sensitive Intellectual Property (IP), such as documentation for making glass molds and customer design files. Over the last few years, digital solutions, devices, and users proliferated in the organization across business functions, increasing the number of users and devices by 60%. IP is the company's competitive advantage, so a stronger and resilient security posture is critical to prevent data leakage and exfiltration by both insiders and external threat actors.



“Being a data-driven manufacturing company, it is of the utmost importance for us to ensure that the data coming in is continuous, secure, and uncompromised, and that we know exactly what is happening in each device. That is one of the things that Armis does extremely well.”

—Sudip Mazumder
CDIO, PGP Glass Private Limited

The company had antivirus, along with an endpoint detection and response (EDR) scanning its IT network but lacked the ability to scan OT and IoT devices and extract detailed insights. Due to design limitations, many of the company's OT systems ran on legacy versions of Windows with no visibility into whether the antivirus software was truly effective on these systems or not.

In addition to those concerns, the company needed to ensure that real-time, reliable data was fed into its energy optimization model, which could use AI and ML to improve efficiency and reduce waste in manufacturing processes.

The Solution

Armis Centrix™ was rolled out in phases, at one plant at a time in India. The deployment was eventually expanded to manufacturing facilities in Sri Lanka. The Armis platform is now part of a holistic ecosystem of technology that feeds into the company's unified energy monitoring system (UEMS) and real-time manufacturing intelligence (RTMI) system. The system collects data from 10,000 sensors that monitor everything from water in the borewell, to the energy in the pit and furnaces. This and other OT data from programmable logic controllers (PLCs) and scanners flows into Armis and then into other tools and systems such as the EDR solution and, eventually, into the security information and event management (SIEM) solution. Armis is able to discover and derive data on external temporary devices, for example mobile phones used by executives and visitors that connect to the corporate network.

Armis supplied the critical missing piece in the company's technology ecosystem: OT data, such as sensor data getting ingested through different integration points including SAP and IoT systems. Since Armis also performs asset management and functions as a configuration management database (CMDB) for all types of devices, including IT and mobile, PGP Glass will be able to sunset other now redundant tools from its network.

PGP Glass has also started to use Armis Centrix™ for VIPR to discover, prioritize, and remediate vulnerabilities in both OT devices and mobile phones. Once integration with the company's SIEM is fully realized, the team will be able to better navigate the sea of alerts, gain greater insights into device security status, and automate remediation processes.

The Results

Armis has greatly improved the situational awareness of all assets connected to the network across the ecosystem and boosted its overall security posture, providing visibility into compliance and patching status of OT systems and Microsoft Window devices. The Armis data flowing from the sensors, gateways, and other OT sources is clean and reliable. This ensures the UEMS and RTMI modules can run properly with the right frequency and volume.

As the team at PGP Glass deepens its familiarity with the Armis dashboards, they are looking at how they can expand the platform across IT as well. Future plans include full adoption of Armis worldwide beyond manufacturing locations to branch offices and even partner sites.

“Until Armis came along, we didn’t have anything as strong or intelligent that could scan the entire network and all our devices—especially OT. With Armis, we started getting those scans. The plan is to expand Armis across all our locations”

—Amit Jha
General Manager and Global
Head IT and Cybersecurity,
PGP Glass Private Limited

“We are building reliable AI models on reliable data,” shares Sudip Mazumder, Global Chief Digital and Information Officer (CDIO) of PGP Glass. He continues, “That is where Armis is doing its work to ensure the devices are visible and operational parameters are visible, which provides us data reliability. We save USD\$2 million equivalent each year through our AI / ML models based on the reliable data from operations. Hence it is so important for us to have both the IT and the OT network running properly and securely.”

\$2 million

USD\$2 million (equivalent value)
in savings each year through
Data Analytics

1720 +

Manufacturing capacity of 1720 +
tons per day

10,000 +

More than 10,000 + OT sensors
monitoring energy consumption



Increased improvement in
production efficiency and energy
efficiency due to reliable real-time
data from Armis



1.888.452.4011
www.armis.com

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization’s cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

