



# Plasser Builds Robust Security Framework Underpinned by Sophos MDR

Plasser India Pvt. Ltd. addresses its growing concerns about defending its business from advanced cyberthreats with a proactive approach to security driven by a powerful suite of security solutions and services from Sophos.

## CUSTOMER-AT-A-GLANCE



**Plasser India. Pvt. Ltd.**

**Industry**  
Manufacturing

**Website**  
[www.plasserindia.com](http://www.plasserindia.com)

**Number of Users**  
750+

**Sophos Solutions**  
XGS Firewalls  
Sophos MDR Complete for Endpoints  
Sophos MDR Complete for Servers

Sophos NDR  
Sophos Wireless APX  
SD-RED  
TAM  
Professional Services

*“Cybersecurity is priority number one for Plasser India, and a growing threat landscape drove us towards a more evolved approach to cybersecurity founded on advanced security products that worked in tandem and an MDR service delivered by expert professionals who have just one key objective – protect Plasser from advanced cyberattacks.”*

Sanjay Srivastava, Plasser India Pvt. Ltd, CIO

Plasser India Pvt. Ltd is a leading manufacturer of the most advanced high-performance machines for train track maintenance, laying, and renewal. It has a 50-year history of developing, manufacturing and exporting track maintenance machines. It delivered its first track machine to the Indian railways in 1965. It also services foreign markets and prides itself on its product quality and efficient after-sales service. As a reputed name in manufacturing, Plasser India has stringent cybersecurity protocols to protect sensitive data and enforce good governance by safeguarding all assets and conforming to industry regulations around cybersecurity. In its continued attempts to ensure the impregnability of its operations, data, and other valuable assets, it decided to leverage the capabilities of Sophos' robust product portfolio and managed detection and response (MDR) service for proactive, always-on protection.

## Challenges

- Keeping up with industry-specific regulations and ensuring that there is no misalignment from a security perspective
- Safeguarding sensitive information and monitoring IT assets 24x7 to ensure a threat doesn't fall through the cracks
- Identify threats swiftly and comprehensively and respond and remediate them before they disrupt operations
- Ensuring there is no weak link in the security chain
- Addressing security concerns with a modern security paradigm

## What critical security concerns drove the need for a more comprehensive and consolidated approach to security?

Like many other manufacturers, Plasser India Pvt. Ltd. was grappling with the intricacies of complying with industry-specific standards such as ISO 27001 and NIST SP 800-171. “The security challenge we faced was not limited to consistently aligning with regulations but also having the flexibility to meet evolving norms quickly and in a sure-footed manner,” said Mr. Srivastava

The company also took its stewardship of sensitive data very seriously and wanted to bolster its security framework to safeguard data, including customer information, employee archives, financial intelligence, and R&D breakthroughs. Plasser India wanted to make data security a key driver in fostering credibility to build customer trust. To do this, it wanted to implement stringent encryption protocols to defend this sensitive data. Another critical challenge was improving network defences by deploying strong network security that fostered a resilient network architecture.

Mr. Srivastava was also aware of the need to initiate a swift response upon threat identification, which would reduce the risk of data breaches. He also wanted to ensure this response was perfectly scripted, immediate, automated, and well-coordinated, wherein multiple security products' capabilities worked simultaneously to ward off threats.

Also, being a large manufacturing company and working with sensitive systems, Plasser India wanted to ensure that personnel were only authorized to access the systems necessary for their roles.

"We saw the need to extend our security team with highly skilled experts who harnessed the power of all the security tools to monitor, investigate, and respond to alerts 24/7, but at the same time, we wanted control costs," says Mr. Srivastava.

## How do you address security concerns by shifting to an optimal approach to securing assets?

Plasser India Pvt Ltd., did not want a multi-vendor approach to cybersecurity and trusted Sophos to deliver end-to-end security across endpoints and network. The company has deployed a variety of Sophos solutions, including XG Firewall, Sophos Wireless APX, SD-RED Sophos NDR (Network Detection and Response), and Sophos MDR Complete for Endpoints and Servers. Together, these solutions deliver powerful protection, visibility, and response to stop known and unknown threats before they access the network or endpoint.

Plasser can now leverage comprehensive access control features to restrict unauthorized system access, synchronized encryption in real-time, protect its software most vulnerable to exploits, and harness advanced threat protection backed by machine learning and behavioral analysis to identify and mitigate known and unknown threats. These solutions work together, share real-time information, and respond automatically to incidents to keep even the most sophisticated threats at bay.

With Sophos Central, the IT team can oversee security policies, configuration, and threats across devices and systems through a single unified interface. This has simplified security management, enhanced visibility, and helped deliver better control over the entire security setup.

With proactive threat hunting conducted by experienced cybersecurity professionals 24x7, Sophos MDR responds to threats before they compromise data or disrupt businesses. Backed by six SOCs, the operations team driving Sophos MDR can execute a full-scale incident response that takes action on behalf of Plasser India to contain and eliminate the threat.



## How has Sophos helped deliver security ROI and facilitated business confidence?

With Sophos, the Plasser IT team is confident that known and unknown threats can be detected and remediated faster. “We benefit from a holistic security symphony that incorporates robust incident response, deploys strong access control mechanisms, allows us to nurture a culture of employee vigilance, and onboard a future-proof approach to security,” says Abinash Kumar – Lead IT Infrastructure.

From a business benefit perspective, the company has mitigated the financial repercussions of security breaches and reduced the risk of business disruptions that result in operational standstill and productivity erosion. Efficient security oversight ensures regulatory compliance, preventing penalties for regulatory non-adherence.

The team now has peace of mind that Sophos’ solutions and MDR service deliver extensive security coverage, thwart cyberattacks, and keep Plasser India’s cybersecurity posture one step ahead of the continuously evolving threat landscape.

“We recommend Sophos’ security portfolio across the network and endpoint to all manufacturers looking to build an impenetrable security ecosystem and experience long-term security ROI,” said Abinash Kumar – Lead IT Infrastructure.

