Zaperon

Identity-centric SSE Platform

CASE STUDY

Protecting IP and Sensitive Data for a Leading Auto-Ancillary Manufacturer

How Zaperon Identity-Centric SSE helped a **₹1,000+ crore** automotive components manufacturer secure **1,000 users** across multiple India locations and stop leakage of drawings, designs, software code, and other sensitive data.



CUSTOMER SNAPSHOT

Industry:
Auto-Ancillary / Automotive Components

Revenue:
₹1,000+ crore

Users:
1,000

Footprint:
Multiple locations across India

Applications:
Microsoft 365, GitHub, SAP

Zero Trust Access | Web Traffic Monitoring | Endpoint DLP | Email DLP | Unified Visibility

Zaperon

Identity-centric SSE Platform

CASE STUDY

The Business Challenge

The customer is a leading Indian auto-ancillary manufacturer with over **₹1,000 crore** in turnover, **1,000 users**, Microsoft 365, and operations across multiple locations. Its engineering and business teams handle highly sensitive data every day — from product drawings and CAD designs to source code, quality documents, commercial files, and customer information.

Where sensitive data lived

1. CAD Drawings & Designs
2. Software Code & Scripts
3. BOMs, Test Reports & Quality Files
4. Customer & Vendor Data
5. Email Attachments & Shared Links
6. Teams / Meet Collaboration Files

Sensitive data was spread across endpoints, Microsoft 365, email, cloud apps, and collaboration workflows — not in one single repository.

What the company was struggling with

- Leakage of drawings and product designs over email and web uploads
- Uncontrolled sharing of source code and commercial files
- Data movement from endpoints without enough visibility
- External collaboration channels creating new exposure paths
- Different user behavior across plants and locations in India
- Pressure to protect IP while maintaining business productivity

Before Zaperon



Zaperon

Identity-centric SSE Platform

CASE STUDY

The Zaperon Deployment

Zaperon deployed its Identity-Centric SSE platform to protect sensitive engineering and business data without disrupting users. The program focused on stopping leakage across the channels employees used every day — while giving the security team one policy framework and one visibility layer.



WHAT WAS IMPLEMENTED

- DLP policies for drawings, designs, source code, customer data, and business files
- Protection for outbound email and attachments in Microsoft 365
- Control over uploads to web applications and unsanctioned destinations
- Endpoint monitoring and prevention for sensitive data movement
- Coverage for collaboration channels including Microsoft Teams and Google Meet
- Centralized audit trails for investigations and compliance reporting

DEPLOYMENT HIGHLIGHTS

1,000 users onboarded	Multiple India locations covered	Microsoft 365, GitHub & SAP integrated	Policy-driven controls by file type and channel	Single console for visibility and response

DEPLOYMENT ROLLOUT

1 **DISCOVER** — Data flows mapped

2 **PILOT** — Policies validated

3 **ROLLOUT** — Users secured

4 **OPTIMIZE** — Controls refined

Zaperon

Identity-centric SSE Platform

CASE STUDY

Business Outcomes

With Zaperon, the customer moved from fragmented protection to a more unified model for safeguarding sensitive data. The deployment helped the organization protect intellectual property, gain visibility across channels, and enforce consistent controls across users, devices, and locations.

1,000
Users Secured

Multiple India Locations Covered

One Unified DLP Policy Framework

Broader Protection Across Email, Endpoints, Web & Collaboration

Before and after

Before Zaperon	After Zaperon
Fragmented controls	Unified policy-driven protection
Limited visibility	Centralized monitoring and audit trails
High risk of IP leakage	Stronger protection for drawings, designs, and code
Manual investigations	Faster incident review and response
Channel-specific security gaps	Consistent controls across email, endpoints, web, Teams and Meet

Key outcomes delivered

- Sensitive design files and drawings better protected from accidental and intentional leakage
- Source code and business-critical data monitored across common exfiltration paths
- Risky email sharing and web uploads brought under tighter control
- Stronger audit readiness through detailed logs and activity trails
- Simplified operations through one integrated SSE platform instead of disconnected point tools

> *Zaperon helped us move from isolated DLP controls to a more unified data protection model aligned to how our teams actually work.*
>
> – CISO, Leading Auto-Ancillary Manufacturer



Zaperon Identity-Centric SSE helps manufacturers protect IP without slowing down operations.