# Securing a Global SaaS Security Platform with Invinsense

## About the Customer

The customer is a leading provider of data-centric security solutions that empower organizations to control and monitor sensitive data usage, even beyond their enterprise perimeter. With a footprint in global enterprises and governments, their SaaS-based platform enables secure collaboration, rights management, and file-level protection across endpoints, cloud, and enterprise applications. Their platform is highly integrated with enterprise ecosystems and operates in multi-cloud environments.

## The Challenge

As a data security SaaS provider, the customer had a dual mandate: protect the core SaaS infrastructure and APIs, and ensure continuous DevSecOps integration for secure product development. With hundreds of customers entrusting them with sensitive data policies, their platform had to be resilient against supply chain attacks, insider threats, API abuse, and advanced persistent threats.

Key challenges included:

| | | |
|---|---|---|
| Protecting sensitive customer data processed across multiple cloud regions. | Preventing lateral movement across containerized microservices and Kubernetes clusters. | Securing a sprawling API surface exposed to enterprise integrations. |
| Aligning product security with ISO 27001, SOC 2, and data protection regulations. | Implementing secure CI/CD pipelines while ensuring rapid innovation. | Managing real-time threat detection and response with limited in-house SOC resources. |

## Deception Outcomes with Invinsense XDR+

- Deployed decoys across cloud infrastructure and test environments, catching 9 unauthorized lateral movement attempts.
- Reduced dwell time of simulated insiders from hours to under 6 minutes through early detection and auto-response.
- Integrated deception telemetry into XDR for improved attack path visibility.

## Compliance Acceleration with Invinsense GSOS

- Automated control mapping and evidence generation for ISO 27001, SOC 2 Type II, and GDPR.
- Reduced internal audit preparation time by 40%.
- Achieved real-time compliance posture visibility across dev, staging, and prod environments.

## DevSecOps Enablement

- Infopercept DevSecOps experts embedded SAST, DAST, and IaC scanners directly into Jenkins pipelines.
- Container image scanning reduced vulnerable image deployments by 54%.
- Runtime policies in Kubernetes prevented unauthorized pod-to-pod communications.

## CTEM in Action with Invinsense OXDR

Invinsense enabled the customer to operationalize Continuous Threat Exposure Management (CTEM) with the following outcomes:

| CTEM Stage | Outcome |
|---|---|
| Scoping | Identified over 370+ exposure points across APIs, cloud functions, and build environments. |
| Discovery | Mapped critical microservices, revealing 28 exposed services in lower environments. |
| Prioritization | Ranked exposures based on blast radius, leading to a 46% reduction in high-risk attack paths. |
| Validation | Simulated real-world attacks, uncovering 8 zero-day misconfigurations across containers. |
| Mobilization | Invinsense and Infopercept teams closed exposures with 72% automation coverage across pipelines and cloud. |

## Solutions Used

- Invinsense XDR for centralized detection, response, threat hunting, and API activity monitoring across cloud workloads and endpoints.
- Invinsense XDR+ to implement deception technologies within staging and production environments, catching lateral movement and privilege abuse early.
- Invinsense OXDR for continuous exposure management across public APIs, containers, and cloud control planes.
- Invinsense GSOS to automate evidence collection, compliance audits, and risk treatment against frameworks like ISO, SOC 2, and GDPR.
- Infopercept DevSecOps Consulting to embed security checks into their CI/CD pipelines, integrating static/dynamic code scans, container image validation, and IaC assessments.

## Key Results

- 65% reduction in attack surface across core SaaS services.
- Improved mean time to detect (MTTD) by 4.5x.
- Achieved zero critical misconfigurations in production over the last two quarters.
- 35% faster audit readiness for SOC 2 and ISO 27001 certifications.
- Prevented 9 lateral movement attempts through deception.
- Integrated security gates across 100% of CI/CD pipelines, enabling secure release cycles.

## Executive Quote

*"With Invinsense, we've not only enhanced our SaaS platform's threat resilience but also streamlined our DevSecOps and compliance workflows. Their CTEM approach gave us continuous visibility into our exposures and helped us act faster with context."*

*– CISO, Global SaaS Security Platform*

Infopercept | INVINSENSE

**About Infopercept** - Infopercept is one of the fastest growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

**Imprint**


**Contact**
sos@infopercept.com
www.infopercept.com/knowledge/casestudy