SwyftComply AI

Fast vulnerability finding ≠ Vulnerability protection

SwyftComply AI closes the discovery-to-protection gap before attackers can exploit it. Autonomous edge patching, human-verified exceptions, audit-ready reporting, on SLA.

★★★★★ **4.9/5** on Gartner Peer Insights · **300+** verified reviews

• THE SWITCH

Attackers exploit with AI. We use AI to find & patch vulnerabilities at machine speed.

Attackers now find and exploit faster than code-level patching can remediate. SwyftComply AI closes that speed mismatch at the edge, autonomously.

• **TRADITIONAL REMEDIATION** | Weeks of exposure, waiting on release cycles

Report → Triage → Backlog → Review → Release

• **SWYFTCOMPLY AI** | **Found and patched in the same cycle**

Discover → Validate → Patch & block → Comply

Protecting thousands of applications. Blocking billions of attacks.

<5 Min	**100%**	**78,000+**	**6,500+**
From DNS change to full protection	Of apps in block mode from day one	Vulnerabilities virtually patched	Customers in 95+ countries

• TRUSTED BY LEADING ENTERPRISES WORLDWIDE

HDFC ERGO · Bandhan Life · TATA CAPITAL · ITC HOTELS RESPONSIBLE LUXURY · TATA POWER

LTM · IndusInd Bank · Bank of India · DANUBE GROUP · TITAN COMPANY

• HOW IT WORKS

Four stages. One SLA.

From first scan to custom policies live at the edge, closed with an audit-ready report. No code change. No backlog.

01 DISCOVER

Context-aware AI pen testing

Multi-model AI agents scan applications for business-logic vulnerabilities, reasoning about your specific workflows, not just signature matching.

02 VALIDATE

Expert governance

Indusface security experts review every finding. False positives eliminated. Severity classified. Each finding mapped to your compliance framework before any policy work begins.

03 PATCH & BLOCK

Library plus bespoke policies

AI agents autonomously apply SwyftComply Policy Engine templates; experts create bespoke policies for exceptional business-logic vulnerabilities. Both are expert-governed before deployment at the edge.

04 COMPLY

Audit-ready report

Virtual patches tested against real traffic. Policies promoted to block mode after expert validation. The cycle closes with a zero-vulnerability report, ready to share with your assessors.

• REAL EXAMPLE

AI finds it. Experts close it.

Loan top-up manipulation

NBFC

Multi-step chain attack, invisible to signature scanners.

The top-up workflow has three steps (eligibility check, apply, disburse), each authenticated and returning 200 OK. AI agents find that changing the amount between the check and disbursement lets a $5,000-eligible customer disburse $50,000. That state desync is invisible to endpoint-by-endpoint scanning.

FIX

Custom policy enforcing amount immutability between eligibility and disbursement, deployed at the edge.

RESULT

Policy live in block mode. Audit-ready for RBI NBFC Master Direction and Fair Practice Code.

• RECOGNIZED AND RECOMMENDED

The analysts agree. So do the buyers.

4.9 ★★★★★

300+ verified reviews on Gartner Peer Insights

100% recommendation, 4 consecutive years

Highest-rated Cloud WAAP

"Our evaluation of SwyftComply AI showed exactly what enterprises need: vulnerabilities closed as fast as they are found, and a report auditors can trust."

Vinayak Godse
CEO
Data Security Council of India (DSCI)

"With SwyftComply AI, findings are patched at the edge as they arrive, so our development teams fix root causes in their normal release cycles instead of constantly reacting."

Nishith Kumar Datta
Head of Information Security
Titan Company Limited

AS FEATURED ON — Gartner · Forrester · GigaOm · S&P Global · IDC · MarketsandMarkets · QKS Group · G2

• ABOUT INDUSFACE

Autonomous application security for the AI era.

Indusface secures the web, API, and AI applications of thousands of organizations across 95 countries. Recognized by Gartner, Forrester, and IDC for its innovation in application security, Indusface meets ISO 27001, SOC 2, PCI DSS, and GDPR standards. Its cloud infrastructure spans Asia, the Middle East, Europe, and North America, enabling low-latency protection and regional data residency.

AppTrana is Indusface's autonomous application security platform. It continuously discovers vulnerabilities, remediates exploitable risks through virtual patching, and protects against DDoS, bot, API, AI, and zero-day attacks. AI-powered intelligence, expert governance, and SLA-backed protection cut the time from discovery to protection, with compliance-ready reports and zero false positives.

Bangalore · Delhi · Mumbai · Vadodara · Dallas

www.indusface.com · sales@indusface.com · support@indusface.com