

Intrusion Prevention System



Overview

JioCloud IPS defends your cloud workloads with real-time, inline threat prevention — without sacrificing performance or uptime. It inspects traffic across Layers 3-7 to detect exploits, alert on anomalies, and take action against malicious behavior before it reaches your application. Using a combination of signature detection, behavior analytics, and real-time threat intelligence, JioCloud IPS blocks threats inline without any performance impact. With a design for cloud-native environments, JioCloud IPS seamlessly integrates into your virtual networks, SOC workflows, and compliance frameworks.

Key Features

- **Deep packet inspection (L3-L7)**
Monitors all levels of network traffic to expose hidden payloads and application layer threats.
- **Signature + anomaly detection**
Uses known threat signatures, then adds behavior analytics to find anomalies and zero-day attacks.
- **Real-time threat blocking**
Stops the malicious activity as soon as it occurs.
- **Inline, low-latency deployment**
Protects the traffic without going offline, or experiencing any latency.
- **Automatic threat intelligence updates**
Automatically pulls the most recent threat intel feed on emerging threats.
- **Granular logging and alerting**
Monitors the environment and generates real-time alerts, while capturing full event logs for investigations and audits.
- **SOC and SIEM integration**
Inputs threat data into a central system to allow for a faster response with further analysis if required.

Benefits

- Real-time prevention of exploits, malware, and zero-day attacks.
- Easier compliance with continuous logging, alerting, and audit trails.
- Inline protection with zero added latency or performance impact.
- Faster triage and response with detailed, contextual alerts.
- Seamless deployment in cloud environments with SOC and SIEM integration

Use Cases

- **Stop advanced attacks**
Detect and stop zero-day exploits, injection attacks, and port scans targeting key backend banking APIs.
- **Respond in real time**
Trigger alerts with rich context to accelerate triage and have report-ready, compliance-friendly reporting.
- **Go beyond firewalls**
Inspect L3–L7 inline traffic to capture important threats you would miss with bolt-on payload-based capabilities.
- **Protect without disruption**
Deploy IPS in a transparent manner in the cloud — no downtime, no performance hit.