JioCloud

SIEM

Overview

JioCloud SIEM brings unified security intelligence to modern hybrid environments - all without the usual complexity. It ingests logs from across your infrastructure, correlates events, and detects real threats in real time. You get built-in support for AWS, Azure, private cloud, and on-prem sources - with no need for extra connectors or plugins. JioCloud SIEM uses pre-configured detection rules, automated incident creation, and real-time dashboards to help your teams cut through the noise and focus on what matters. With our advanced feauters, you stay compliant, reduce time-to-detection, and respond faster - all from a single console.

Key Features

- **Real-time detectors**
  Continuous monitoring and detection of security events.
- **Threat intelligence feeds**
  Real-time threat intelligence feeds allow for detection and response to emerging threats.
- **Event correlation**
  Correlates security events across multiple systems.
- **Alert and notification**
  Automates alerts and notifications across multiple channels.
- **Incident management**
  Provides tools that manage and track security incidents, from detection to resolution.
- **Dashboard and reports**
  Interactive rich interface dashboards and reports.
- **Multi-tenancy and RBAC**
  RBAC enables organizations to define and manage user access permissions.
- **Multi-cloud support**
  Supports multiple cloud infrastructures.
- **Standard and custom rules**
  Pre-configured and customizable security rules enables quick onboarding.

JioCloud

Benefits

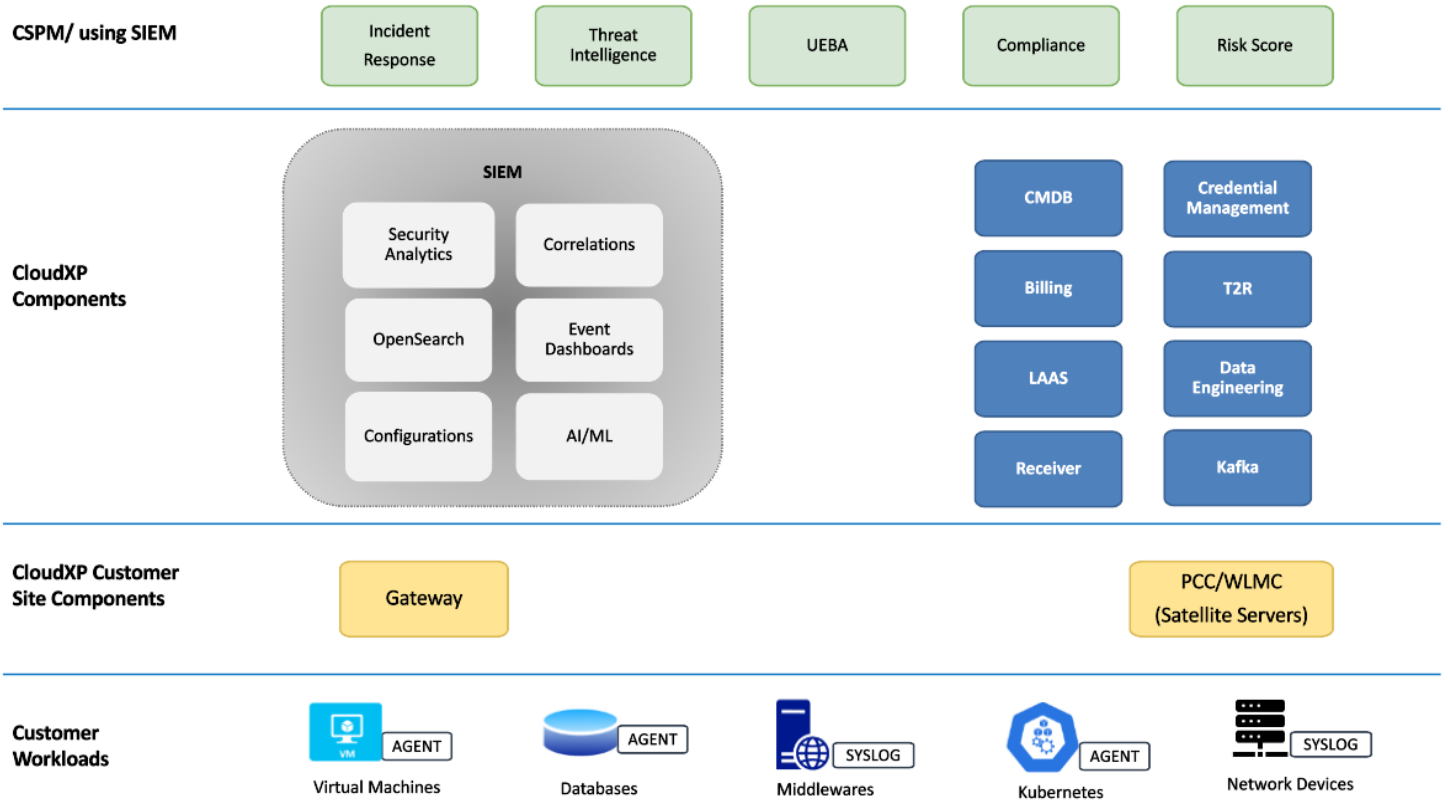
- **Faster detection, faster response**
  Identify and act on real threats faster with real-time detection and automated workflows.
- **90% less alert noise**
  Smart correlation and contextual enrichment reduce triage time - and analyst fatigue.
- **Complete security visibility**
  Track every log, event, and anomaly across your hybrid and multi-cloud stack in one place.
- **Security that scales with you**
  No matter your size or setup, JioCloud SIEM adapts to your environment - without complex integrations.

Technology Support

Technology Category	Technology Name
Operating System	Windows, Linux, Ubuntu, RHEL
Network	Radware WAF, Cisco ASA, Palo Alto, Cisco FTD, TrendMicro Deep Security
Databases	MSSQL, MySQL, Postgres, MongoDB
Application	CloudXP
Containers	Kubernetes

JioCloud

Architecture Diagram



Use Cases

- **From alert to action - without the lag**
  A security analyst receives an alert from JioCloud SIEM. It's already enriched with threat intel, correlated with past activity, and auto-classified based on severity. With a single click, an incident is created, and dashboards reflect the event in real time.

- **Catch the breach before It happens**
  Using AI, JioCloud SIEM flags an unusual login pattern across geographies. A potential credential compromise is stopped before the attacker can move laterally or escalate privileges.

- **Stay compliant, always**
  From automated audit logs to real-time SLA tracking, compliance isn't a scramble - it's built in. Reports can be shared with internal teams or regulators with full traceability.