



# Keep Your Cloud Apps and Infrastructure Secure and Compliant

F5® Distributed Cloud App Infrastructure Protection (AIP)'s, formerly known as Threat Stack, high-efficacy threat detection uses supervised learning to uncover known and unknown threats to cloud infrastructure. With 24/7/365 SOC support, we're an extension of your security team, letting you execute better remediation.



## USE CASES

- Cloud Intrusion Detection
- Compliance
- Insider Threat Detection
- Incident Response
- Vulnerability Assessment
- Secure Applications and Microservices

# Detect Vulnerabilities and Threats in Real Time, with Context and Workflow to Speed Remediation

Because applications and APIs are only as secure as the infrastructure they run on, Distributed Cloud AIP uses rules, supervised machine learning, managed services and more to give you the most high-efficacy alerts for vulnerabilities and threats, allowing you to remain secure and compliant.

## Rich Telemetry Collection

Distributed Cloud AIP provides the industry's most comprehensive cloud security and compliance telemetry collection across the full cloud infrastructure and application stack.

## Real-Time Risk Detection and Compliance

We provide pre-built, customizable rulesets for detecting known security and compliance risk, enabling you to accelerate compliance with all major frameworks including SOC 2, PCI, HIPAA, GDPR, ISO 27001, and SOX, along with the automated reports you need for audit purposes.

## Supervised Learning Detection-In-Depth

Distributed Cloud AIP with ThreatML™ combines rich telemetry and advanced supervised machine learning models to enable security teams to quickly detect, prioritize, and respond to both known and unknown vulnerabilities and threats.

## SecOps Experts

Our Security Operations Center (SOC), including Distributed Cloud AIP Insights and Distributed Cloud AIP Managed Security Services, help you proactively identify risk and respond to threats in real time with our dedicated in-house SOC experts and security analysts actively monitoring your cloud environment 24/7/365.

*"Working with [Distributed Cloud AIP] provides us with the expertise, tools, and roadmap we need to keep our team aligned while executing an effective cloud security strategy. Their highly experienced Security Engineers work with our Security and Operations teams to optimize the company's platform so we can best leverage its automation, real-time alerting, and investigative capabilities for our unique environment."*

**Ken Leeser, CISO at Chrome River**

## FULL STACK SECURITY OBSERVABILITY

### Application

Monitor for vulnerabilities and block attacks against applications, microservices, and APIs

### Orchestration

Monitor for risky behavior and misconfigurations in Kubernetes

### Container

Deploy as a container for automated security and trace suspicious activity across Docker containers

### Host

Host-based intrusion detection with out-of-the-box and customizable rulesets

### Cloud Management Console

Apply behavioral detection to CloudTrail API logs

## DISTRIBUTED CLOUD AIP HELPS YOU

### Reduce Risk

Together our industry-leading cloud security telemetry, robust rules engine, ML-based vulnerability, risk, and anomaly detection, and human expertise helps you identify patterns of risky behavior, increases your likelihood of detecting a breach, helps eliminate both false negatives and false positives (for high-efficacy alerts), and significantly reduces your time to respond.

### Securely Leverage the Cloud

Build trust with your customers that their data is safe, while you build trust between teams in your organization. When security's goals are aligned with the rest of the organization, everyone wins.

### Achieve DevSecOps Observability and Integration

Distributed Cloud AIP extends security observability across the entire software development lifecycle including both build-time and runtime environments, enabling you to seamlessly integrate Development, Security, and Operations teams.

## Full Stack Security and Compliance

### HIGH-EFFICACY THREAT DETECTION

Distributed Cloud AIP monitors all layers of the infrastructure stack from the cloud management console, hosts, containers, orchestration, and applications. You gain the deep observability you need to identify and head off threats, maintain compliance, and move forward securely with your cloud deployments and strategy.

### Actionable Context

- Contextualized signals provide real-time alerts of risky behavior and indicators of compromise
- Proactive risk reduction across every layer of your infrastructure and application stack
- Supervised learning-based behavioral analysis identifies internal and external threats
- Faster incident response with real-time threat detection and alerting

### Flexible Consumption

Alerts and telemetry can be consumed in whatever way fits best with your security or DevOps workflow, whether that's in our platform, a third-party tool or storage solution, or through co-managed services in our Distributed Cloud AIP Managed Security Services program.

## Continuous Cloud Compliance

Leverage pre-built rulesets that map to compliance controls continuous compliance to regulators, auditors, and customers, including these compliance types:



- ISO 27001
- GDPR
- HIPAA
- PCI
- SOC 2
- SOX

## DISTRIBUTED CLOUD AIP'S MANAGED SERVICES


### Distributed Cloud AIP Insights—Make Data-Driven Decisions with Curated Analytics and Personalized Advisory

With Distributed Cloud AIP Insights, one of our expert Security Engineers will curate data on your behalf to help you understand patterns of risky behavior from the results of your ongoing activity across the Distributed Cloud AIP. You'll also receive support with third-party integrations and advanced rule tuning for your use of the platform.

### Distributed Cloud AIP Managed Security Services—Monitor for Potential Security Incidents


With industry-leading Distributed Cloud AIP Managed Security Services, our in-house Security Engineers monitor your environment 24/7/365, alerting you to potential incidents and helping you understand what happened. Our experts leverage the automation, real-time alerting, and unparalleled investigative capabilities of the Distributed Cloud AIP, expanding the expertise, scope and resources of your DevSecOps team.

#### CYBERSECURITY PARTNERSHIPS



aws partner network  
Advanced Technology Partner  
Containers Competency  
Security Competency

#### TECHNOLOGY INTEGRATIONS



puppet slack graylog  
docker Ansible OpsGenie  
pagerduty CHEF SALTSTACK  
VictorOps splunk

## Threat Stack: Now Part of F5

Threat Stack is now F5 Distributed Cloud App Infrastructure Protection (AIP). If you'd like to learn more about this solution, the company's Security Operations Center (including Distributed Cloud AIP Managed Security Services and Distributed Cloud AIP Insights), and more, feel free to contact our cloud security and compliance experts.

**Let our experts take your cloud security worries off your shoulders, so you can get down to business. To learn more or to schedule a demo, [visit our website](#) today.**

