DATA SHEET

Continuous Compliance for Cloud Infrastructure and Applications

Common Frameworks and Regulations to Achieve and Maintain Compliance

F5® Distributed Cloud App Infrastructure Protection (AIP), formerly known as Threat Stack, helps organizations complete cloud compliance certifications and satisfy audit requests by providing pre-built and customizable rulesets for SOC 2, PCI DSS, HIPAA, and ISO 27001.

Observe Telemetry Across Your Infrastructure

Start your compliance journey with Distributed Cloud AIP through telemetry collection from your cloud infrastructure stack across cloud management consoles, hosts, containers, Kubernetes, and applications.

Fast and Seamless Classification

Deploy the Distributed Cloud AIP agent, leverage a combination of custom compliance rulesets and ThreatML™, immediately gain valuable insights on compliance events in your environment.

Automatically Report on Compliance

Monthly reports delivered within the application collect and surface critical information specific to your compliance frameworks needed to accelerate and pass compliance audits.

Maintain Your Compliance Posture

Distributed Cloud AIP Insights and Managed Security Services support continuous compliance and allow you to satisfy requirements for 24/7/365 security and compliance monitoring by leveraging our expert SOC team to triage high-severity issues, investigate alerts on your behalf, and provide remediation recommendations.

WE HAVE TO MAKE IT EASY FOR AN ASSESSOR TO VALIDATE THAT WE'RE DOING WHAT WE SAY WE'RE DOING, AND [DISTRIBUTED CLOUD AIP] PROVIDES INSIGHTS INTO WHO IS DOING WHAT, WHERE, AND WHEN—ALONG WITH AN AUDIT TRAIL AND REPORTS THAT CAN BE PASSED ALONG TO AN AUDITOR.

– BRIAN DAIELY,
CO-FOUNDER AND CTO
AT STRATASAN

Key Compliance Features

File Integrity Monitoring

Continuously track if a critical file has been accessed, opened, copied, moved, created, or modified in a way that appears suspicious.

User Behavior Analysis

Track abnormal or suspicious user behavior including file copies, privilege escalations, policy violations, and context such as the user who made the change and the command-line process that was performed.

Detailed Audit Logs

In-depth audit trails capture every detail about the operating system as it runs, ensuring you have complete visibility for compliance audits and incident investigation.

> *"[Distributed Cloud AIP] enabled us to meet several PCI requirements simultaneously with one solution."*
>
> **Kevin Eberman, Director of Operations at MineralTree**

A Hardened Cloud Security Strategy for Seamless Compliance

Distributed Cloud AIP compliance support is driven by our technology and services that enable our customers to achieve full stack cloud security across their workloads. With Distributed Cloud AIP, customers can leverage the business benefits of the cloud while maintaining visibility and control across their workloads.

Services

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

With Distributed Cloud AIP Insights, a Distributed Cloud AIP Security Engineer 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 Advanced. You'll also receive support with third-party integrations and advanced rule tuning for your use of the platform.

TECHNOLOGY INTEGRATIONS

puppet slack graylog
docker ANSIBLE OpsGenie
pagerduty CHEF SALTSTACK
VictorOps splunk>

Distributed Cloud AIP Managed Security Services Monitor for Potential Security Incidents

With Distributed Cloud AIP Managed Security Services, our in-house Distributed Cloud AIP Security Engineers will 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 Managed Security Services.

Full Stack and Compliance Visibility

- **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 and out-of-the-box rulesets
- **Cloud Management Console:** Integrates with cloud service providers for runtime monitoring of cloud account activity

> *"[Distributed Cloud AIP] helps us automate our general security and auditing process, but the best part is eliminating manual evidence collection for compliance."*
>
> **Harrison Hunter, CTO at SaaS Startup**

Actionable Context

- Contextualized signals provide real-time insight into risky behavior and indicators of compromise
- Proactive risk reduction across every layer of your infrastructure and application stack
- Robust rulesets can be customized to fit your use case, such as labeling rules to match a compliance framework or setting rules that do not create alerts
- Rulesets, behavioral analysis, and ML-based anomaly and vulnerability detection work together to identify internal and external threats
- Faster incident response with real-time threat detection, context, and remediation recommendations, reducing mean-time-to-know (MTTK) and mean-time-to-respond (MTTR)

Flexible Consumption

Distributed Cloud AIP's rich security and compliance insights can be consumed within your existing security, compliance and DevOps workflow, whether that's in the Distributed Cloud AIP console, a third-party tool, or through co-managed services with Distributed Cloud AIP Managed Security Services and Distributed Cloud AIP Insights.

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 and compliance worries off your shoulders, so you can get down to business. To learn more or to schedule a demo, visit our website today.