Simplify SOC 2 Compliance Management

Mapping SOC 2 Requirements

F5® Distributed Cloud App Infrastructure Protection (AIP), formerly known as Threat Stack, Feature–Continuous Monitoring

Distributed Cloud AIP ensures that you're never left in the dark when it comes to knowing what's happening in your infrastructure and applications. The Distributed Cloud AIP solution automatically monitors and records all the activity happening in your cloud, providing you with the instruments you need to effectively maintain a healthy security posture.

Distributed Cloud AIP:

- Continuously monitors your cloud to identify and evaluate security threats and unusual system activity—both known and unknown
- Provides granular insight into running systems and control effectiveness
- Allows you to identify areas of risk based on host software package installations
- Monitors for internal and external system users accessing infrastructure, software, and data

SOC 2 Requirement

Distributed Cloud AIP's monitoring capabilities impact the following SOC 2 requirements:

- Monitoring Activities (CC4.1, CC4.2)
- Control Activities (CC5.1)
- System Operations (CC7.1, CC7.2, CC7.4, CC7.5)
- Change Management (CC8.1)

Distributed Cloud AIP Feature–Alerting

The Distributed Cloud AIP solution monitors and records the activity happening in your cloud, sounding alarms if suspicious behavior is detected. Get notified instantly of anomalous behavior indicating unauthorized access to customer data so you can respond instantly.

Distributed Cloud AIP will alert you on:

- Threats that may impair system security, availability, processing integrity, or confidentiality
- Suspicious filesystem, account, and configuration activity
- Anomalous activity across host servers, containers, and the cloud management console

SOC 2 Requirement

Distributed Cloud AIP's alerting capabilities impact the following SOC 2 requirements:

- Risk Management (CC3.3)
- Logical and Physical Access Controls (CC6.1, CC6.6)
- System Operations (CC7.1)
- Additional Criteria for Processing Integrity (PI1.3)

Distributed Cloud AIP Feature–Investigate and Verify

Determine whether an event is a true threat using Distributed Cloud AIP's detailed auditing system. Our audit trails provide you with the intelligence you need to understand an attack's impact so you can answer the who, what, where, when, and how in order to make informed decisions on how to respond in the event of a compromise.

Distributed Cloud AIP provides audit logs detailing:

- Additions or removals of system components
- Unauthorized modifications of data and configurations
- Insight into system activity useful for early threat identification
- Root cause analysis intelligence to enhance post-incident response

Distributed Cloud AIP provides you with deep visibility into the underlying kernel—the source of truth—where system activity can't be faked. Distributed Cloud AIP gives you instant, comprehensive visibility into your full cloud infrastructure stack and sounds the alarms if suspicious behavior is detected.

SOC 2 Requirement

Distributed Cloud AIP's investigation and verification capabilities impact the following SOC 2 requirements:

- Risk Assessment (CC3.2)
- Logical and Physical Access Controls (CC6.2)
- System Operations (CC7.1, CC7.2)

Distributed Cloud AIP Feature–Maintain and Evaluate

Distributed Cloud AIP offers co-managed services to help supplement your infosec and operations teams. Our expert Security Analysts are available to help document findings and recommended actions, as well as analyze your risk profile over time.

Distributed Cloud AIP services come in two forms:

- Distributed Cloud AIP Managed Security Services provides 24-7 eyes-on-glass coverage with Security Analysts investigating and validating high severity alerts in your cloud environment.
- Distributed Cloud AIP Insights helps guide work to reduce risk and harden infrastructure by analyzing the data generated by your Distributed Cloud AIP implementation. Reviews occur on a regular basis with Distributed Cloud AIP Security Analysts.

SOC 2 Requirement

Distributed Cloud AIP Managed Security Services and Insights services impact the following SOC 2 requirements:

- Control Activities (CC 5.3)
- Logical and Physical Access Controls (CC6.8)
- System Operations (CC7.3)

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.