Simplify PCI DSS Compliance Management

Mapping PCI DSS Requirements

F5 Distributed Cloud App Infrastructure Protection Feature–Continuous Monitoring

F5® Distributed Cloud App Infrastructure Protection (AIP), formerly known as Threat Stack, 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:

- Provides granular insight into running systems and control effectiveness.
- Monitors at the kernel level, as well as critical points in the cardholder data environment, providing a level of monitoring beyond that of basic intrusion detection.
- Is always on and always watching, ensuring applications are protected.

PCI DSS Requirement

Distributed Cloud AIP's monitoring capabilities impact the following PCI DSS requirements:

- **Requirement 1:** Install and maintain a firewall and router configuration to protect cardholder data (1.5)
- **Requirement 6:** Develop and maintain secure systems and applications (6.3, 6.5, 6.6)
- **Requirement 10:** Track and monitor all access to network resources and cardholder data (10.6)
- **Requirement 11:** Regularly test security systems and processes (11.4, 11.5)
- **Requirement 12:** Maintain a policy that addresses information security for all personnel (12.10)

Distributed Cloud AIP Feature–Alerting

Distributed Cloud AIP monitors and records all the activity happening in your cloud and sounds the alarm if suspicious behavior is detected. Get notified instantly of anomalous behavior indicating unauthorized access to cardholder data so you can respond immediately.

Distributed Cloud AIP will alert you on:

- Suspicious filesystem, account, and configuration activity.
- Unauthorized exposure or modification of data and unauthorized use of cloud resources.
- Data, configuration, and activity changes within areas of high risk.
- Violations of policies and procedures.

PCI DSS Requirement

Distributed Cloud AIP's alerting capabilities impact the following PCI DSS requirements:

- **Requirement 6:** Develop and maintain secure systems and applications (6.1, 6.2, 6.4, 6.5, 6.7)
- **Requirement 7:** Restrict access to cardholder data by business need to know (7.2, 7.3)
- **Requirement 8:** Assign a unique ID to each person with computer access (8.1, 8.7)
- **Requirement 11:** Regularly test security systems and processes (11.2, 11.5, 11.6)

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 lets you address:

- Audit logs and alerting on unauthorized exposure or modification of data and configurations.
- Log and security event reviews for all system components to identify anomalous activity.
- Creation of an independent repository for storing alerts that is supplemental to log information.

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.

PCI DSS Requirement

Distributed Cloud AIP's investigation and verification capabilities impact the following PCI DSS requirements:

- **Requirement 10:** Track and monitor all access to network resources and cardholder data (10.1, 10.2, 10.3, 10.5, 10.6, 10.7, 10.8)
- **Requirement A.1:** Protect the cardholder data environment (A.1.3, A.1.4)

Distributed Cloud AIP Feature–Maintain and Evaluate

Distributed Cloud AIP offers co-managed services to help supplement your infosec and operations teams. Our security analysts are available to help document findings and recommended actions, as well as improve your security posture over time.

Distributed Cloud AIP services come in two forms:

- Distributed Cloud AIP Managed Security Services provides 24x7 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 implementation. Reviews occur on a regular basis with Distributed Cloud AIP Security Analysts.

PCI DSS Requirement

Distributed Cloud AIP Insights and Managed Security Services impact the following PCI DSS requirements:

- **Requirement 12:** Maintain a policy that addresses information security for all personnel (12.2, 12.5, 12.10)

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.