Simplify HIPAA Compliance Management

Mapping HIPAA 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 provides you with the instruments you need to effectively maintain a healthy security posture in the cloud.

Distributed Cloud AIP:

- Monitors for suspicious file system, account and configuration activity
- Provides granular insight into running systems and control effectiveness
- Allows you to identify and report on risky behaviors and suspicious commands

HIPAA Requirement

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

- General Rules (164.306(e))
- Administrative Safeguards (164.308(a)(1)(ii)(A), 164.308(a)(5)(ii)(C), 164.308(a)(6)(i), 164.308(a)(6)(ii))
- Technical Safeguards (164.312(a)(2)(iv))

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 PHI, so you can respond immediately.

Distributed Cloud AIP will alert you on:

- Changes in data, configurations and login activities that are indicators of compromise
- Violations of policies and procedures

- Unauthorized exposure or modification of data
- Tampering with encryption, applications or keys

HIPAA Requirement

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

- General Rules (164.306(a))
- Administrative Safeguards (164.308(a)(1)(i), 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(C), 164.308(a)(1)(ii)(D), 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(A), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(6)(i), 164.308(a)(6)(ii))
- Technical Safeguards (164.312(a)(1), 164.312(c)(1), 164.312(c)(2), 164.312(e)(1), 164.312(e)(2)(i))

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:

- Continuously monitors activity across your servers, identifying potential threats
- Documents security incidents, allowing you to mitigate future threats
- Provides detailed information from Linux and Windows Server system activity that can be used to detect and respond to issues

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.

HIPAA Requirement

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

- Administrative Safeguards (164.308(a)(8), 164.308(a)(1)(ii)(D))
- Technical Safeguards (164.312(b), 164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i))

Distributed Cloud AIP Feature–Maintain and Evaluate

Distributed Cloud AIP Managed Security Services and Distributed Cloud AIP Insights 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 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 implementation. Reviews occur on a regular basis with Distributed Cloud AIP Security Analysts.

HIPAA Requirement

Distributed Cloud AIP Managed Security Services and Insight services impact the following HIPAA requirements:

- General Rules (164.306(e))
- Administrative Safeguards (164.308(a)(8))
- Policies and Procedures and Documentation Requirements (164.316(b)(1)(ii))

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.