Getting Help with ISO 27001 Compliance

This document describes the security controls, policies, practices, and incident response program that customers can use to keep infrastructure secure and compliant with F5® Distributed Cloud App Infrastructure Protection (AIP), formerly known as Threat Stack.

Distributed Cloud AIP's monitoring helps track the following changes and anomalous behaviors:

- Abnormal user actions including file copies, privilege escalations, and policy violations
- Unauthorized critical file modifications and access using File Integrity Monitoring (FIM)
- Suspicious network activity, such as command and control connections and external scans into the environment
- Discovery of vulnerable packages on the workload as well as CVE (Common Vulnerability and Exposures) information and remediation tactics
- API calls that do not follow AWS best practices and CIS benchmarks for any AWS Service that feeds into CloudTrail (AWS ONLY)

Along with early behavior-based breach detection, Distributed Cloud AIP greatly reduces Mean Time to Know and Mean Time to Respond (MTTK and MTTR), which ensures the highest level of security, incident response, and compliance alignment.

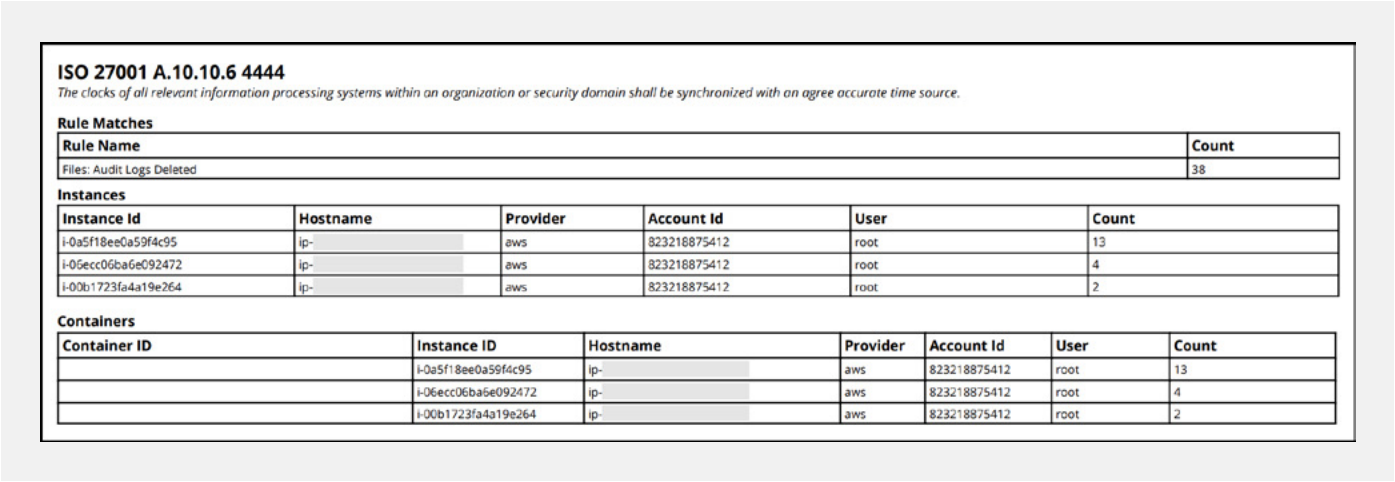
Key Security and Compliance Controls

Distributed Cloud AIP provides ISO-27001-specific compliance classifiers, which trigger alerts immediately upon any behavior that runs outside of the ISO 27001 framework. By combining behavioral data from the host, cloud management console, and containers, security and operations teams can achieve full visibility across cloud infrastructure. The compliance classifiers contains the following classifications and rules:

Severity 1: Highest Severity Requiring Instant Response—Reviewed and remediated immediately.

Severity 2: Medium Severity—Warning-level alerts for daily internal review to determine the necessary response.

Severity 3: Low Severity—Do not require immediate action. Captured for review and compliance verification.



ISO 27001 A.10.10.6 4444

The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agree accurate time source.

Rule Matches

Rule Name	Count
Files: Audit Logs Deleted	38

Instances

Instance Id	Hostname	Provider	Account Id	User	Count
i-0a5f18ee0a59f4c95	ip-	aws	823218875412	root	13
i-06ecc06ba6e092472	ip-	aws	823218875412	root	4
i-00b1723fa4a19e264	ip-	aws	823218875412	root	2

Containers

Container ID	Instance ID	Hostname	Provider	Account Id	User	Count
	i-0a5f18ee0a59f4c95	ip-	aws	823218875412	root	13
	i-06ecc06ba6e092472	ip-	aws	823218875412	root	4
	i-00b1723fa4a19e264	ip-	aws	823218875412	root	2

Figure 1: Custom Sample Daily Compliance Alert Report

Response Workflow with Distributed Cloud AIP

Distributed Cloud AIP combines multiple detection and assessment techniques including host-based intrusion detection for Linux and Windows Server, file integrity monitoring, Docker and Kubernetes monitoring, Linux vulnerability assessment, and CloudTrail monitoring so customers can detect early signs of a security incident and systematically reduce risky behavior over time.

We provide deep contextual information in correlation with each alert to help security and operations teams quickly determine whether behavior is malicious so they can respond appropriately. We also offer compliance classifiers aligned with SOC 2, PCI, HIPAA, and MPAA to help achieve and continuously maintain compliance.

Detect

When risky or anomalous behavior is detected, Distributed Cloud AIP alerts customers in real time and provides contextual information,including the process that was run, who ran it, the location, the severity level, and more.

For example,the following alert shows attempted data exfiltration, which is classified as a Severity 1 alert and indicates that there is a high possibility of a bad actor. Customers can see basic information about the alert such as the source IP, command, user, and event type to help better understand what caused the alert, so that they can take action on it.

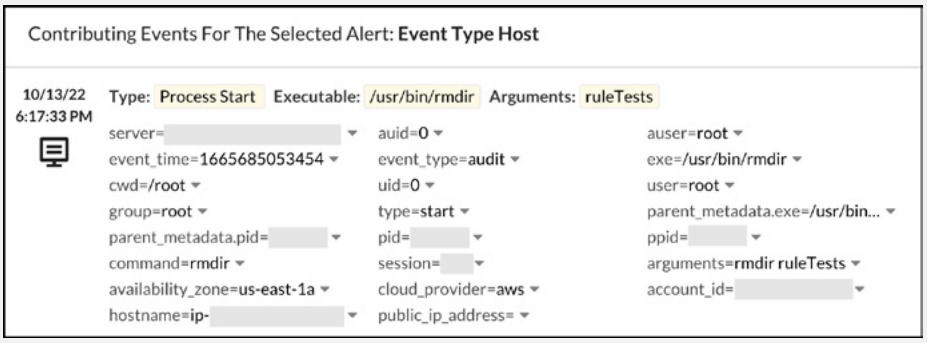


Figure 2: Event Type Host Alert

Investigate

By clicking further into this data exfiltration alert in the Distributed Cloud AIP solution, customers can investigate exactly what this user did, see any associated events, see what other commands they ran in the session, and understand whether it came from outside the network or was an insider threat.

One of the contributing events in this situation is a connection with a known malicious IP in Ukraine, so clearly this user was able to connect through a known vulnerability and remotely execute commands that gave them access to secret compliance files.

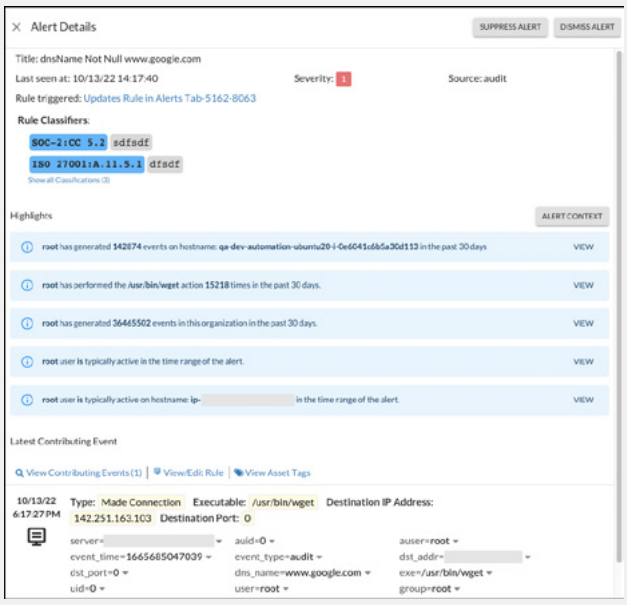


Figure 3: Investigate Alert Details

Remediate

Within seconds of this command being executed, customers can determine that this is an incident they need to respond to immediately before the bad actor is able to access sensitive data or cause damage.

Wrap Up

Distributed Cloud AIP can help security and operations teams satisfy the parameters of most compliance standards by continuously monitoring important files, firing alerts in real time as soon as someone touches those files, and tracking exactly what that bad actor did leading up to the alert. With in-depth contextual data at hand, customers can gain the best understanding of security events and can put proper measures in place to continuously harden the compliance and security posture of its cloud infrastructure.

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.