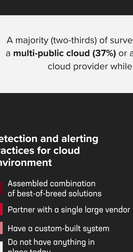
Approaches to Threat Monitoring and Detection for Cloud-Based Enterprises

How are companies managing the transition to the cloud and keeping up with compliance issues and managing security in public and hybrid cloud environments?

Gatepoint Research surveyed **200 executives*** from various industries to find out–and their responses were very insightful.

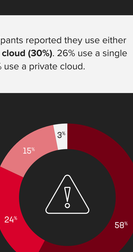
Cloud Threat Monitoring Strategies are Complex

What percentage of workloads are in the cloud?



- More than 80%
- 41% to 60%
- 20% or less
- 61% to 80%
- 21% to 40%

How are you hosting your infrastructure in the cloud?

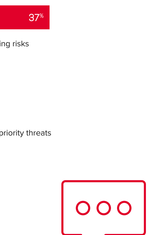


- Multi-public cloud
- Hybrid cloud
- Single cloud provider
- Private cloud

A majority (two-thirds) of survey participants reported they use either a **multi-public cloud (37%)** or a **hybrid cloud (30%)**. 26% use a single cloud provider while only 7% use a private cloud.

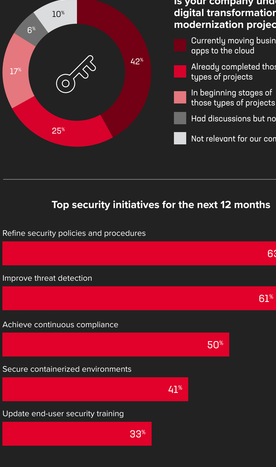
Detection and alerting practices for cloud environment

- Assembled combination of best-of-breed solutions
- Partner with a single large vendor
- Have a custom-built system
- Do not have anything in place today



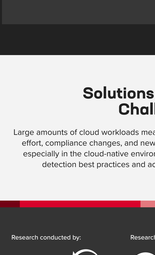
Top Challenges and Issues

Common security and compliance process complaints



LOOKING AHEAD

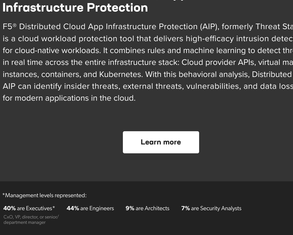
Solutions to Address Challenges



Is your company undertaking digital transformation/app modernization projects?

- Currently moving business apps to the cloud
- Already completed those types of projects
- In beginning stages of those types of projects
- Had discussions but no actions
- Not relevant for our company

Top security initiatives for the next 12 months



Survey participants report that the following cloud **security solution features would be most useful** to their team:

- **46%** Anomaly detection via machine learning
- **46%** Recurring scans
- **41%** Customizable rules
- **32%** Managed SOC escalations

Solutions to Address Challenges

Large amounts of cloud workloads mean organizations are struggling with manual effort, compliance changes, and new threats to apps, APIs, and infrastructure, especially in the cloud-native environment. They want to improve their threat detection best practices and achieve compliance in an easier way.

Research conducted by: GATEPOINT RESEARCH

Research sponsored by: F5

About F5 Distributed Cloud App Infrastructure Protection

F5® Distributed Cloud App Infrastructure Protection (AIP), formerly Threat Stack, is a cloud workload protection tool that delivers high-efficacy intrusion detection for cloud-native workloads. It combines rules and machine learning to detect threats in real time across the entire infrastructure stack: Cloud provider APIs, virtual machine instances, containers, and Kubernetes. With this behavioral analysis, Distributed Cloud AIP can identify insider threats, external threats, vulnerabilities, and data loss risk for modern applications in the cloud.

Learn more

*Management levels represented:

40% are Executives* **44%** are Engineers **9%** are Architects **7%** are Security Analysts

*CxO, VP, director, or vertical/department manager