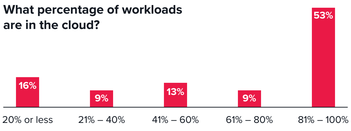
threat stack
Part of F5

Monitor Threats and Stay Compliant in the Cloud: Success Strategies

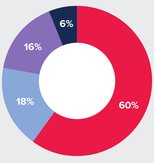
How do companies keep on top of the complexity of threat monitoring where compliance and auditing requirements are constantly evolving and demand ever-increasing focus and time?

Gatepoint Research surveyed **200 cloud security and compliance experts*** in eCommerce, EdTech, FinTech, HealthTech, and Media-On-Demand (MOD) industries to find out – and their responses were quite insightful.

Threat Detection in the Cloud: A Top Priority



The majority of survey participants reported they either use a single cloud provider (37%) or a multi-public cloud (36%). Just under 25% leverage a hybrid cloud; only 5% use a private cloud.



Detection and alerting practices for cloud environment

- Best-of-breed combination of solutions
- Custom-built system
- Partnership with a single large vendor
- Nothing in place currently

Top Security and Compliance Process Challenges

What keeps cloud security experts up at night?

Looking Ahead in Cloud Security

Top security initiatives for the next 12 months

- **51%** Improve threat detection
- **46%** Identity and access management
- **46%** Achieve continuous compliance
- **43%** Refine security policies and procedures
- **31%** Secure containerized environments
- **26%** Update end-user security training

Those surveyed cite the following features in a cloud security solution would be the most useful to their team: Anomaly detection via machine learning (46%), recurring scans (46%), customizable rules (41%), and managed SOC escalations (32%).

Factors that drive investment in security technology

- Regulatory/Audit Changes **(61%)**
- Security Excellence **(59%)**
- Cost control **(52%)**

Conclusion

Large amounts of cloud workloads mean organizations are struggling with manual effort, compliance challenges, 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.

Threat Stack can help.

Research conducted by: GATEPOINT RESEARCH

Research sponsored by: threat stack Part of F5

About Threat Stack, part of F5

Threat Stack, a part of F5, 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, Threat Stack can identify insider threats, external threats, and data loss risk for modern applications in the cloud.

LEARN MORE

Management levels represented:

19% CxO or VP **17%** Director **38%** Manager **26%** Engineer or Architect