Enterprise Strategy Group™
by TechTarget

Cloud Detection and Response

Increasingly dynamic cloud environments are presenting visibility challenges for security. Indeed, the majority of organizations claim that lack of access to physical networks, the dynamic nature of cloud-native applications, and elastic cloud infrastructure create blind spots, making security monitoring challenging. Additionally, nearly all organizations experienced a cloud security incident in the last year, which can result in application downtime, unauthorized access, data loss, and compliance fines. TechTarget's Enterprise Strategy Group recently surveyed IT and cybersecurity professionals responsible for evaluating or purchasing cloud security technology products and services to gain insights into these trends.

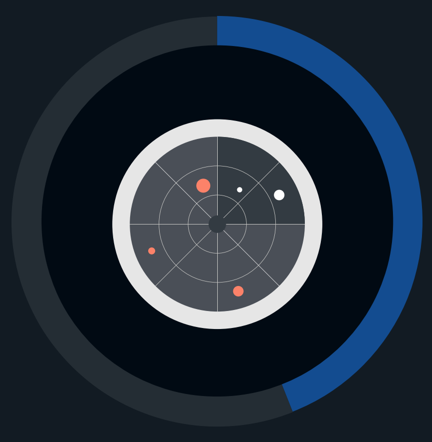
Notable findings from this study include:

60%

of organizations ***lack complete confidence*** **in the level of visibility they have in their cloud application environment.**

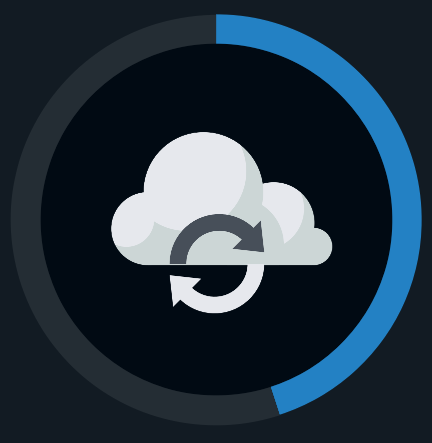
88%

of security professionals believe that the differences between cloud applications and the rest of their applications require different security skills, tools, and processes.



44%

of security professionals believe that it is more difficult to conduct threat detection and response in cloud environments.

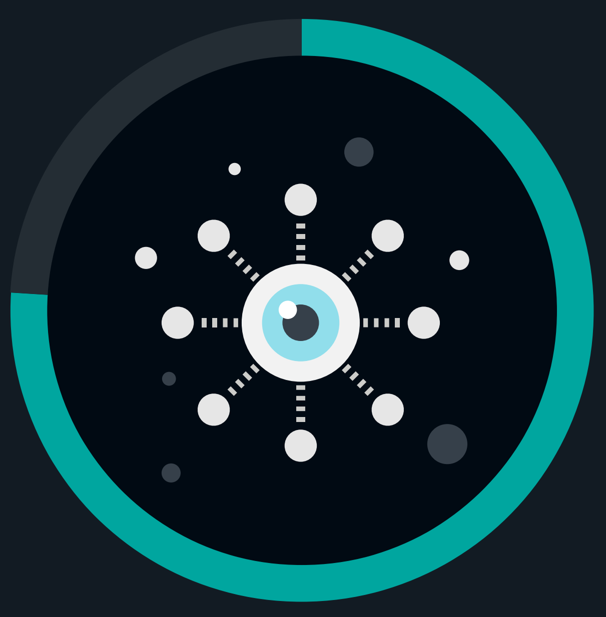


45%

of organizations report their SOC and cloud engineering teams share cloud detection and response responsibilities evenly.

57%

of organizations that use agent-based monitoring for their cloud workloads consider these solutions to be completely effective.



76%

of organizations believe they need to ***significantly*** **increase their visibility and investigation capabilities for applications for which agents cannot be deployed.**

For more from this Enterprise Strategy Group study, read the full research report, ***Cloud Detection and Response.***

LEARN MORE

Source: Enterprise Strategy Group Research Report, *Cloud Detection and Response*, December 2023.