



Comprehensive Visibility and Reduced MTTK in a Complex Environment

Customer Problem

Genesys is the global provider of PureCloud, an all-in-one Cloud Contact Center Solution. To enhance scalability, agility, and operational efficiency, Genesys transitioned to AWS, leveraging services such as EC2, S3, CloudTrail, Elastic Load Balancing, and Relational Database Service (RDS)—creating a new environment that was 100% cloud-native and microservice-based.

Following the transition, the operations and security teams faced the challenge of ensuring host-level visibility across their ephemeral, dynamic environment. After failing to achieve this using OSSEC, Genesys looked for a purpose-built solution that could continuously monitor and alert across elastic cloud and hybrid environments, settling on the F5® Distributed Cloud App Infrastructure Protection (AIP), formerly known as Threat Stack, solution.

The Solution

As soon as they deployed Distributed Cloud AIP, Genesys gained full stack security observability and critical visibility into the process of spinning up new microservices on new servers, going through the configuration management process, and tearing down old servers. Genesys was also able to leverage the ability to baseline “normal” behavior throughout their environment, rapidly contextualize signals from across the entire cloud infrastructure, and deliver real-time alerts when any anomalous activity occurred. Using data collected from all actions/behaviors taking place in their critical environments, Genesys was able to fine-tune their alerts and achieve a 75% reduction in time to investigate a potential incident, shifting them from a less reactive to a more proactive approach to securing their infrastructure.



Founded
1990

Headquarters
Daly City, CA

Industry
Customer Experience

Employees
6,000+

Outcomes and Benefits

Genesys has seen major gains since adopting AWS and Distributed Cloud AIP. Where AWS has brought agility and cost-efficiencies, the Distributed Cloud AIP solution enables Genesys to see contextualized and actionable security telemetry from across their infrastructure correlated in one place. With continuous monitoring of Genesys' environment, the team can focus on other work, confident they'll be alerted if anything suspicious occurs. In short, this cybersecurity solution has enabled strong security while decreasing time to detection, resource requirements, and hours wasted chasing security events across a complex environment.

"[Distributed Cloud AIP] saved us hours previously spent chasing down security events, eliminating the need to hire another security resource."

Jarrod Sexton, Lead Information Security Engineer, Genesys

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 worries off your shoulders, so you can get down to business. To learn more or to schedule a demo, [visit our website](#) today.

