Thundra

Observability and security for serverless applications

Benefits

- Discover bottlenecks - Detect issues up to 50% faster by visualizing the serverless architecture aggregated by traces, metrics, and logs viewed in a single pane.
- Troubleshoot in minutes - Reduce mean time to resolution (MTTR) by up to 60% with Thundra's actionable real-time alerts. Assess business impact and take rapid actions.
- Reduce costs – Identify resource expenses and improve resource utilization where necessary to reduce costs up to 40%.
- Granular security and compliance - Monitor security and compliance across dev, test, and runtime using whitelists, blacklists, and anomaly detection for AWS Lambda functions and serverless architecture.

Product overview

Built for debugging, observability, and security, Thundra provides deep security and performance insights into serverless-centric workloads. Thundra enables software teams to quickly improve the workflows of serverless applications, where data is spread across managed services and third-party APIs. Thundra eases the debugging process with distributed and local tracing of serverless applications using AWS Lambda functions. Thundra improves MTTR and consolidates disparate tools to monitor applications, detect issues, alert, debug, troubleshoot, reduce costs, improve security posture, and prove compliance.

Product features

Monitor performance and cost of serverless workflows

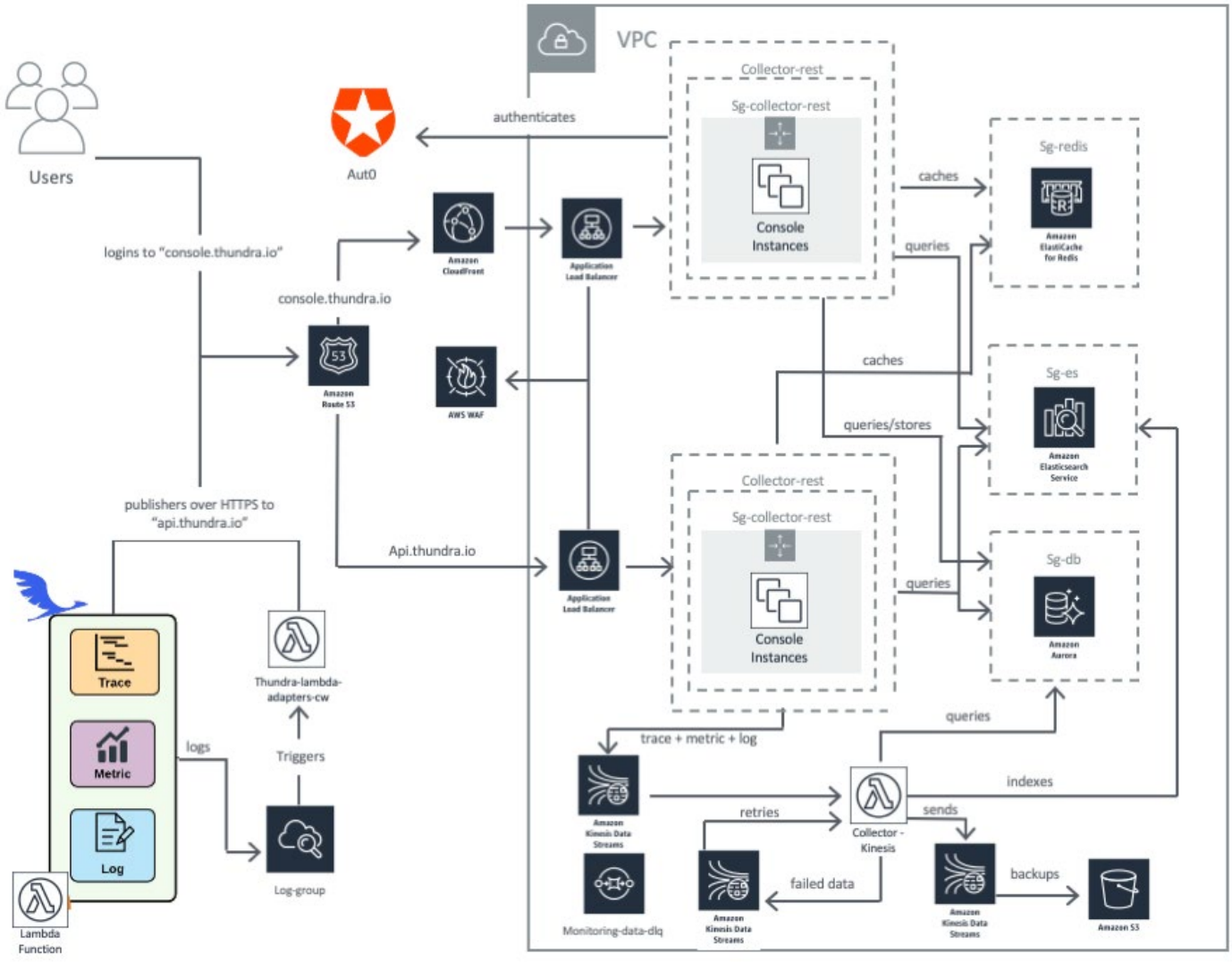
Thundra monitors all of your serverless architecture composed of functions, third-party APIs, and AWS or non-AWS resources. It also provides an architectural view of all the services used by a serverless application with insights into performance and cost. Thundra brings distributed and local tracing to allow software teams to track serverless transactions with insights into the application code to accelerate MTTR.

Close the doors for potential security events

Software teams accelerate delivery by incorporating security into their continuous integration and continuous delivery (CI/CD) workflows and runtime environments. Behavior anomalies are proactively detected across AWS Lambda functions. By detecting and whitelisting or blacklisting 3rd parties, Thundra helps to improve serverless application compliance and can aid in the reduction of incidents.

How it works

Thundra manages application health by combining debugging with automated distributed tracing and security for serverless and containers. Thundra offers more detailed observability for AWS Lambda environments with aggregated logs, metrics, and traces. By identifying bottlenecks, Thundra helps provide additional visibility into unexpected situations for rapid actions and fast debugging throughout the application lifecycle.



Solution available in [AWS Marketplace]