Architecture and Software Development

Life Cycle Guide

ManageEngine Cloud Security Plus

ManageEngine Cloud Security Plus is a log monitoring tool for public cloud platforms. This tool gives complete visibility into your AWS (cloud trail, s3, elb), Azure (activity logs, nsg), Salesforce (event logs, audit trials) and Google cloud infrastructures. The comprehensive reports, easy search mechanism, and customizable alert profiles enable you to track, analyze, and react to events happening in your cloud environments. Thus, facilitating the smooth functioning of your business in a secure and protected cloud.
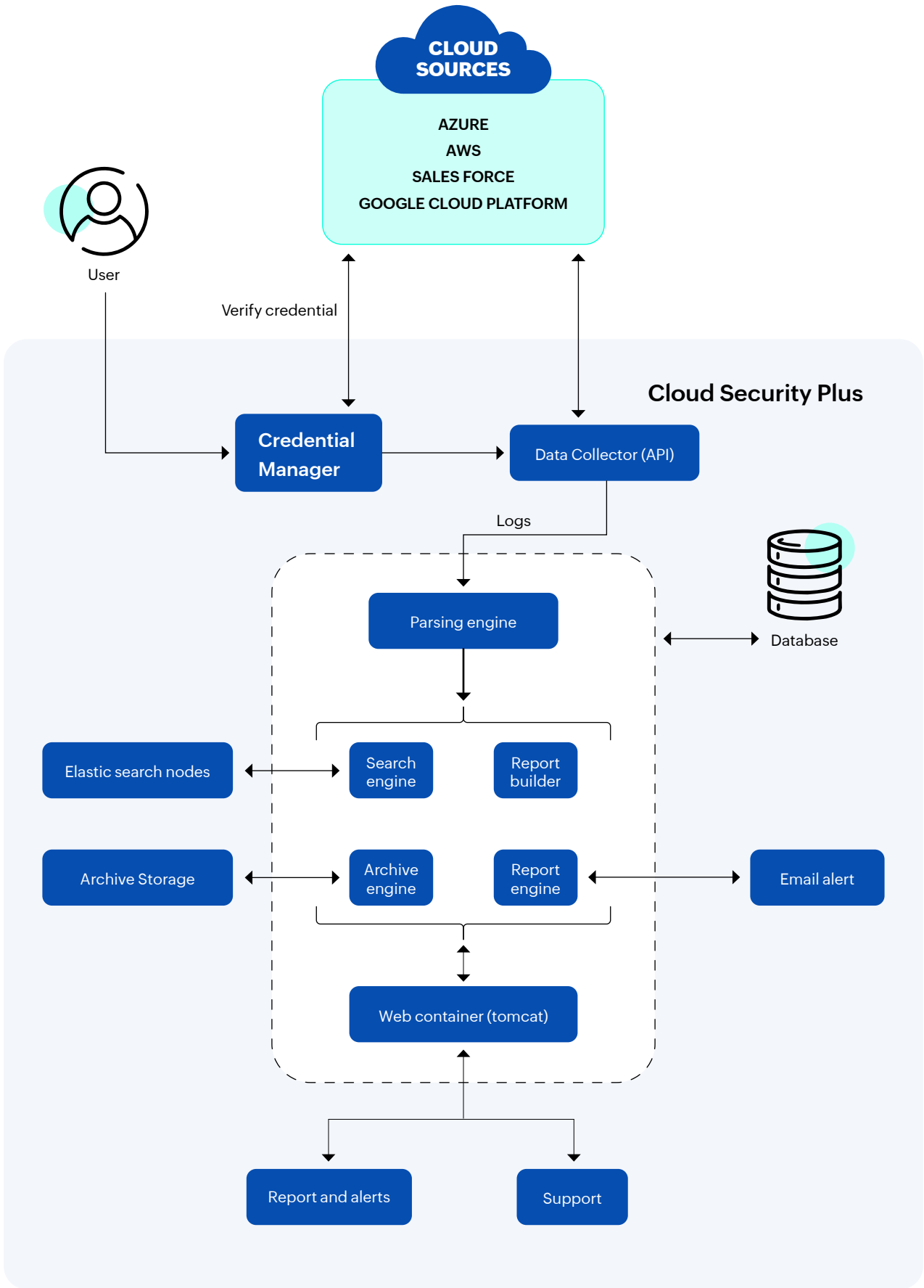
Architecture

- **Data collector:** Collects log data from various cloud sources configured in the product via API calls at scheduled time intervals.

- **Parsing engine:** Filters and normalizes raw logs into a standard format.

- **Database:** Postgres is used to store user configuration details and other log source information.Elastic search is efficiently used to store all the logs collected from the configured cloud source.

- **Report builder:** Processes the raw and normalized logs to build all the predefined reports.These reports enable you to monitor every activity in your environment. Cloud Security Plus generates and sends out scheduled reports, and it exports reports when needed.

  Additionally, an interactive dashboard provides a bird's-eye view of data represented graphically.
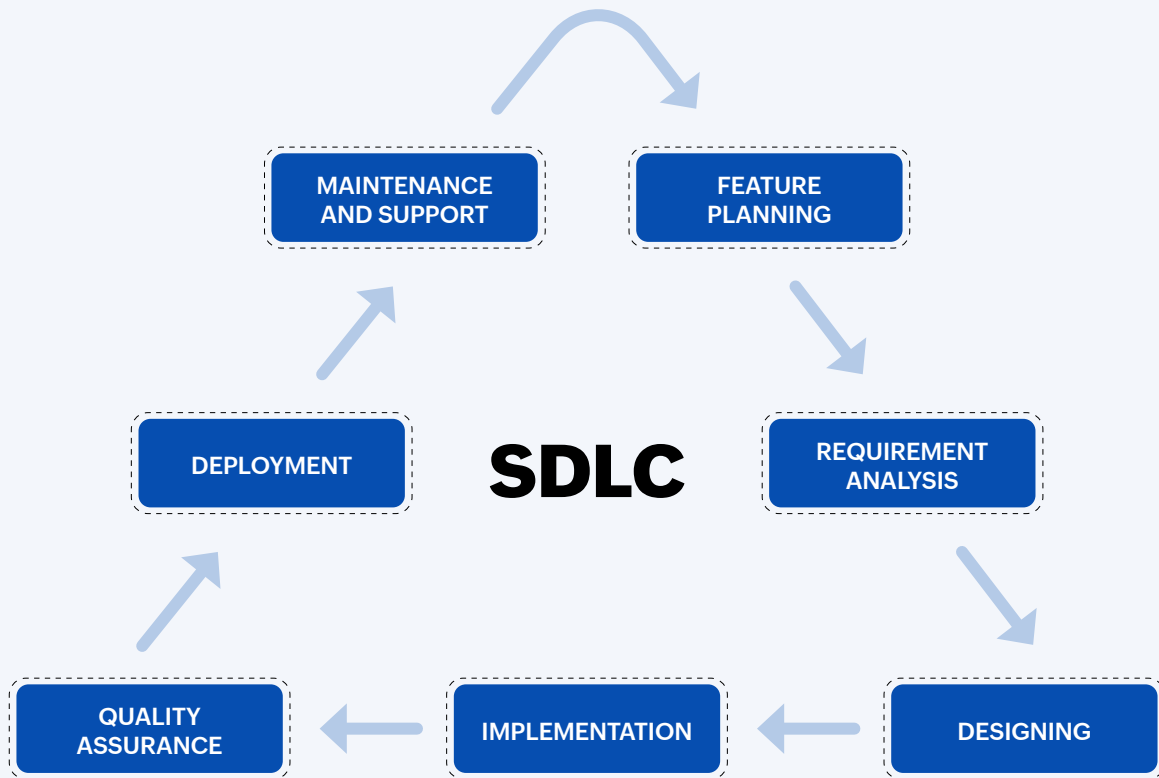
- **Alerts:** To make the end user aware of plausible threats in their cloud environment, automated notifications are sent via email when unusual activities, anomalous trends, and other security threats occur.

  Based on how serious the event is, alerts are prioritized and categorized so that you can immediately focus on critical events to prevent a security breach.

- **Log search engine:** The search engine, powered by Elasticsearch, is employed to store parsed logs from all the configured cloud sources. It swiftly searches through millions of logs in seconds, delivering customer-required logs and information.

- **Archive engine:** ES indices would be archived after the user specified number of days.

ManageEngine
Cloud Security Plus

CLOUD SOURCES

AZURE
AWS
SALES FORCE
GOOGLE CLOUD PLATFORM

User

Verify credential

Cloud Security Plus

Credential Manager

Data Collector (API)

Logs

Parsing engine

Database

Elastic search nodes

Search engine

Report builder

Archive Storage

Archive engine

Report engine

Email alert

Web container (tomcat)

Report and alerts

Support

Software development lifecycle

MAINTENANCE AND SUPPORT

FEATURE PLANNING

DEPLOYMENT

SDLC

REQUIREMENT ANALYSIS

QUALITY ASSURANCE

IMPLEMENTATION

DESIGNING

ManageEngine
Cloud Security Plus

Cloud Security Plus, the cloud security monitoring component of Log360, manages log data from Amazon Web Services, Microsoft Azure, Salesforce and Google Cloud Platform. With an elaborate security analytics dashboard, extensive insights on suspicious cloud events and real-time alerts, Cloud Security Plus helps track user activity, protect sensitive data and ensure cloud security. For more information about Cloud Security Plus, visit manageengine.com/cloud-security/.

$ Get Quote   **↓ Download**