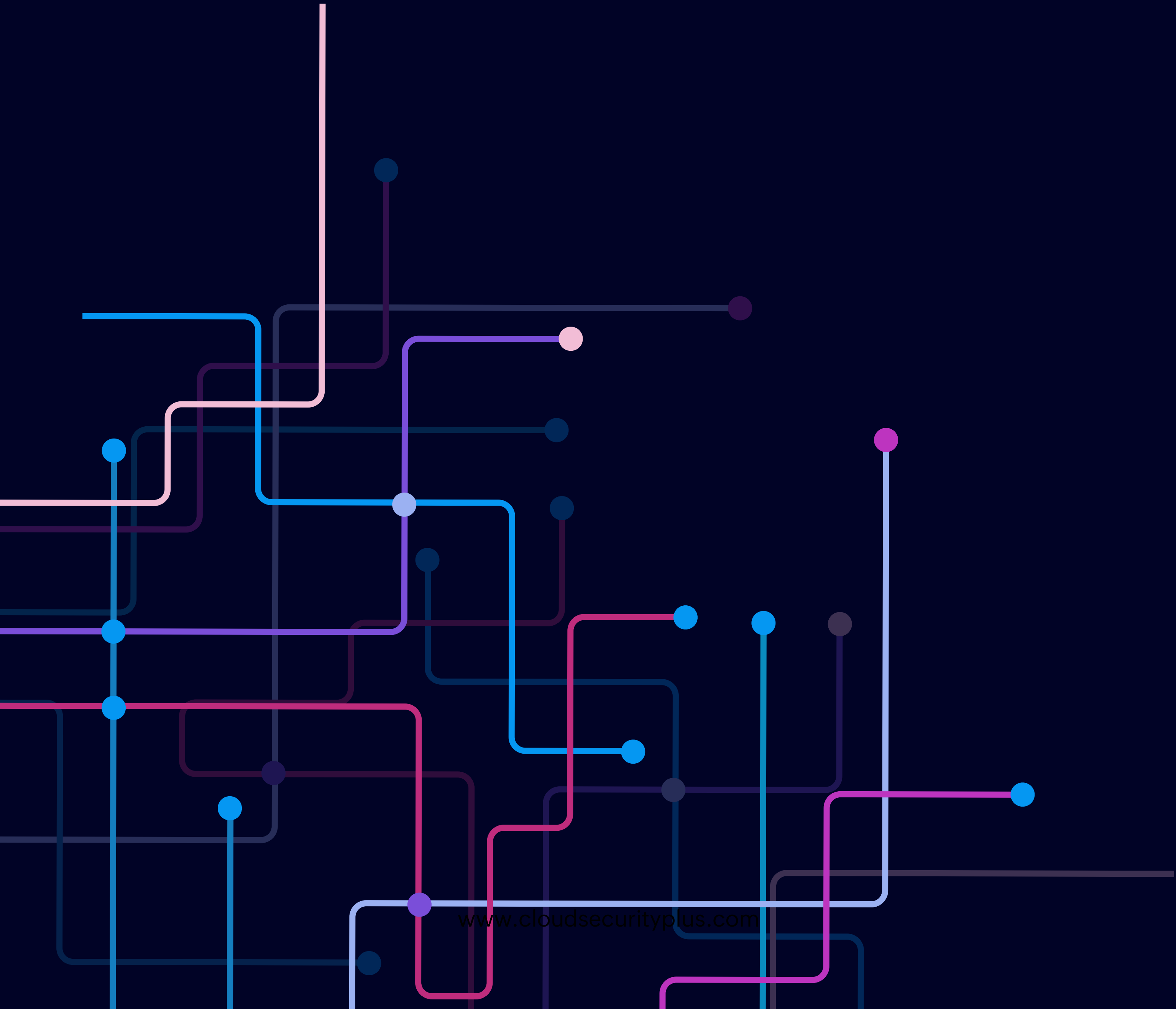
ManageEngine
Cloud Security Plus

Data integrity techniques and security measures adopted by Cloud Security Plus



www.cloudsecurityplus.com

Cloud Security Plus has several mechanisms to ensure that the security and integrity of log data is maintained at every stage of the log management process. This document elaborates on the data integrity methods adopted by Cloud Security Plus to secure log data that is collected, monitored and analyzed.

Log collection

- **Security of logs in transit:**

  Different security and encryption techniques such as **TLS, AES-256** and more are employed to secure the logs that are in transit. Based on the type of log data, the techniques vary.

  1. **Encryption:**

     a. **In transit:** Any data transfer to the server happens using HTTPS. Further, during data transfer TLS and strong ciphers are employed to enhance security.

     b. **At rest:** Users can set HTTPS as the default protocol for all communication from the web console.

     c. **Database protection:** The product database can be accessed only by providing instance-specific credentials and is limited to local host access. The passwords stored in a database in the customer's environment are one-way hashed using bcrypt and are filtered from all of our logs. As bcrypt hashing algorithm with per-user-salt is used, it would be exorbitant and heavily time-consuming to reverse engineer the passwords.

- **Security of logs at rest:**

  Logs at rest refer to the log data that are stored in the Elasticsearch (ES), databases, and temp files. To ensure the integrity of archived logs, **AES-256** encryption is used.

- **ES Data In-transit:**

  The integrity of ES data while transiting using TLS is ensured using **Search Guard ES Plugin.**

Other Security measures

- **Secure web communication:**
  Cloud Security Plus is a web-based solution with a web client that can be accessed from anywhere in the network. Enabling HTTPS protocol ensures that all web communication is secure.

- **Role Based Access Control (RBAC):**
  Cloud Security Plus allows you to compartmentalize your data among the product's technicians. Two access levels are provided: Administrator and Operator, in order to limit user access and control to specific features and device information. This way, you can ensure that data is accessed only by authorized personnel. Administrator will have access to all the tabs. Admins can allow and restrict access to reports, search and alerts tabs to the operator.

- **Technician actions:**
  Cloud Security Plus provides a built-in option to generate the audit trail of all user actions performed in the product. This allows you to ensure accountability within the solution itself.

- **Session termination after idle time:**
  With Cloud Security Plus, you can set up a session expiry time and if the session is idle for more than 10 minutes (which is the minimum time), then the session will be terminated. Users can change the default setting of 30 minutes for session expiry to 10 minutes by following the below steps:

1. Login to Cloud Security Plus web-console as an Admin.
2. Navigate to **Settings > Product Settings > Connection Settings.**
3. In the **Session Expiry Time Field** provide value as **10.**

Log archival

- **ES index archival:**

  Cloud Security Plus allows to archive ES index after specific number of days. You can archive ES index by following the below steps:

  1. Login to Cloud Security Plus as an Admin.
  2. Navigate to **Settings > Admin Settings > Alerts/Logs.**
  3. In the **Archive ES index after**, field provide the specific number of days.

Contact support for more details

For further details, please contact support support@cloudsecurityplus.com.